DISEÑO E IMPLEMENTACIÓN DE UNA HERRAMIENTA DINÁMICA PARA LA ADMINISTRACIÓN DE RIESGOS EN EL PROCESO DE COMPRAS PARA LA EMPRESA TRANSELCA S.A E.S.P.

JORGE ALVAREZ VIVIESCAS

KAREN GUERRERO POLO

JONHATAN VELASCO NIÑO

TONY VILLALBA GARRIDO

UNIVERSIDAD DE LA COSTA –CUC-

ESPECIALIZACIÓN EN AUDITORIA A LOS SISTEMAS DE INFORMACIÓN

BARRANQUILLA–ATLANTICO-

2012

DISEÑO E IMPLEMENTACIÓN DE UNA HERRAMIENTA DINÁMICA PARA LA ADMINISTRACIÓN DE RIESGOS EN EL PROCESO DE COMPRAS PARA LA EMPRESA TRANSELCA S.A E.S.P.

JORGE ALVAREZ VIVIESCAS

KAREN GUERRERO POLO

JONHATAN VELASCO NIÑO

TONY VILLALBA GARRIDO

Trabajo de grado como requisito para optar

Por el título de Especialista en Auditoria a los Sistemas de Información

DIRECTOR

MBA. JAIRO SALAZAR PÉREZ

DOCENTE DE ESPECIALIZACIÓN –CUC-

UNIVERSIDAD DE LA COSTA –CUC

ESPECIALIZACIÓN EN AUDITORIA A LOS SISTEMAS DE INFORMACIÓN

BARRANQUILLA –ATLANTICO-

2012

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Barranquilla, 14-12-2012

AGRADECIMIENTOS

En primer lugar a Dios, que siempre nos guía y nos da la fortaleza suficiente para afrontar la vida, dándonos nuestra recompensa, de acuerdo a nuestros actos.

A nuestras familias que aun en los momentos de adversidad están apoyándonos, amigos y profesores que estuvieron presentes en éste proceso de aprendizaje.

Al Ing. Víctor Montaño Ardila por su constante apoyo e interés en el tema objeto de investigación.

A Transelca S.A. ESP, maravillosa organización que nos abrieron las puertas y confió en nuestro profesionalismo para ejecutar este proyecto.

RESUMEN

Actualmente la administración de riesgos es vista a nivel mundial como un asunto crítico que concierne a los niveles directivos de las empresas. Un programa mal diseñado puede dejar vulnerable a una organización frente a percances que retrasen el alcance de sus metas. La administración de riesgos es una función de muy alto nivel dentro de la organización para definir un conjunto de estrategias que a partir de los recursos busca en el corto plazo mantener la estabilidad financiera de la empresa, protegiendo los activos e ingresos. Y en el largo plazo, minimizar las pérdidas ocasionadas por la ocurrencia de dichos riesgos. El éxito en los negocios exige ser excelente en la gestión del riesgo, por eso los administradores de riesgos deben ser inteligentes en la gestión del riesgo. El administrador debe tomar conciencia del riesgo, distinguir las distintas naturalezas del riesgo para conocer la forma de mitigarlo o bien minimizar sus efectos y optimizar los recursos empleados en la gestión, todo ello forma parte de la Inteligencia de la gestión empresarial. Su objetivo es añadir el máximo valor a todas las actividades de la empresa de forma sostenida. Para ello introduce una visión común de los aspectos positivos, oportunidades, y de los aspectos negativos, las amenazas, que pueden afectar al proyecto empresarial, aumentando la probabilidad de éxito y reduciendo la probabilidad de fallo, así como la incertidumbre acerca de la consecución de los objetivos.

En años recientes, el término "Administración de Riesgos Empresarial" se ha acuñado para distinguir la administración de riesgos tradicional de una visión más completa y proactiva de riesgos operacionales en la organización. La pregunta es, ¿cómo puede el administrador de riesgos empresarial ayudar a las áreas operativas a tomar riesgos y utilizar esto como una ventaja competitiva para sus compañías? Para poder tomar riesgos inteligentemente, la organización necesita construir y evaluar riesgos en toda la organización desde una falla de energía hasta huracanes y administración de datos o amenazas al activo de su marca.

---

http://www.aon.com/colombia/products-and-services/risk-services/risk-services.jsp

http://www.aon.com/colombia/products-and-services/risk-services/erm.jsp

http://200.26.134.109:8092/unisucre/hermesoft/portal/home_1/rec/arc_2129.pdf

http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/2GestiondeRiesgos(AR)_es.pdf

http://www.pascualbravo.edu.co/site/images/stories/administrativo/calidad/fundamentos_gestion_riesgo.pdf

ABSTRACT

Currently risk management is viewed worldwide as a critical issue concerning the executive levels of business. A poorly designed program can leave an organization vulnerable to mishaps that delay against the scope of their goals. Risk management is a very senior role within the organization to define a set of strategies from resources (physical, human and financial, information) looking in the short term to maintain the financial stability of the company, protecting assets and income. And in the long run, minimize the losses caused by the occurrence of such risks. Success in business requires to be excellent in risk management, so risk managers should be intelligent risk management. The administrator must be aware of the risk, to distinguish the different natures of the risk to know how to mitigate or minimize their effects and optimize the resources dedicated to management, all part of the intelligence business management. Its objective is to add maximum value to all activities of the company steadily. It introduces a common vision of the strengths, opportunities, and negative aspects, threats that may affect the business project, increasing the likelihood of success and reduce the probability of failure and the uncertainty of achieving objectives.

In recent years, the term "Enterprise Risk Management" has been coined to distinguish the traditional risk management a more comprehensive and proactive operational risk in the organization. The question is, how can the risk manager to help business operational areas to take risks and use this as a competitive advantage for their companies? To take risks intelligently, the organization needs to build and evaluate risks throughout the organization from a power failure to hurricanes and data management or active threats to their brand.

---

http://www.aon.com/colombia/products-and-services/risk-services/risk-services.jsp

http://www.aon.com/colombia/products-and-services/risk-services/erm.jsp

http://200.26.134.109:8092/unisucre/hermesoft/portal/home_1/rec/arc_2129.pdf

http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/2GestiondeRiesgos(AR)_es.pdf

http://www.pascualbravo.edu.co/site/images/stories/administrativo/calidad/fundamentos_gestion_riesgo.pdf

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

1. INTRODUCCIÓN

Es importante reconocer primeramente que en todas las empresas independientemente el sector económico, las políticas de seguridad de la información deben asegurar cuatro aspectos fundamentales que son:

- Autenticación
- Controles
- Integridad
- Confidencialidad

A partir de estos pilares básicos surgen componentes esenciales que constituyen y ayudan a establecer el análisis de riesgos del macro-proceso de adquisición de bienes y/o servicios de la empresa de servicios públicos Transelca S.A. ESP.

Teniendo en cuenta lo anterior, se pretende desarrollar una herramienta dinámica que organice los procesos en función a los riesgos inherentes que éstos presenten, determinando de ésta forma, los riesgos puros o inherentes a cada proceso, el tratamiento o medidas de administración, y los riesgos residuales.

El planteamiento tendrá como base el mapa de riesgos estratégicos de la empresa, previamente definido y administrado por la organización, el cual trata de la implementación sistemática de un conjunto de acciones tendientes al manejo óptimo de los riesgos en todos los procesos. "Este manejo tiene como gran objetivo garantizar la continuidad de los negocios de la organización". El ciclo de la Gestión Integral de Riesgos tiene como punto de partida el mapa estratégico corporativo y competitivo del grupo empresarial. Este Ciclo comprende:

- Identificación
- Evaluación
- Manejo
- Monitoreo
- Comunicación
- Divulgación en todas las etapas.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Diseñar e implementar una herramienta dinámica para la administración de los riesgos y controles en el proceso de compras para Transelca S.A. E.S.P., buscando mantener un adecuado ambiente de control.

2.2 OBJETIVOS ESPECÍFICOS

- Diseño de una metodología y herramienta dinámica para gestionar riesgos y controles por procesos.
- Implementar Herramienta dinámica en el proceso de adquisición de bienes y/o servicios de Transelca S.A. ESP.
- Evaluar el control interno existente con la herramienta automatizada
- Establecer controles para la mitigación de riesgos potenciales en el proceso de adquisición de bienes y/o servicios de Transelca S.A. ESP

3. JUSTIFICACIÓN

En la actualidad, las grandes organizaciones tienen muy presente que la gestión integral de riesgos constituye una práctica inherente a la actividad empresarial, buscando preservar la integridad de los recursos empresariales, aumentar la ventaja competitiva y establecer políticas adecuadas que contribuyan con la continuidad del negocio, frente a los diferentes riesgos a los cuales se encuentran expuestas.

Es por ello que se resalta la importancia de un adecuado análisis de riesgo y posterior a ello, gestionar y administrar los riesgos, evaluando de esta forma el control interno que la organización tenga, mostrando así, el compromiso de estar constantemente preparado ante una eventualidad adversa, Transelca S.A. ESP no es ajena a la gestión de riesgos, puesto que tiene claramente definida las políticas que competen a éste tema; pero, carece de herramientas que contribuyan a manejar de manera optima la gestión de riesgos en los procesos internos de la organización.

También cabe resaltar, el continuo crecimiento del Grupo Empresarial ISA y su filial Transelca S.A. ESP, lo cual hace necesario definir un marco general para la gestión y administración de riesgos por procesos de manera automatizada, orientado a satisfacer las necesidades, asegurar el mejor resultado técnico y económico para las filiales del Grupo, buscando objetividad en los resultados.

Dada la importancia, la intención de este proyecto, es complementar las políticas de gestión integral de riesgos de Transelca S.A. ESP, brindando al analista de riesgos una herramienta automatizada, que le permita manejar una adecuada administración de riesgos de una manera organizada y eficiente. La solución aquí planteada, busca entregar de manera objetiva y oportuna informes que permitan dar apoyo a las decisiones de la alta gerencia.

4. PLANTEAMIENTO DEL PROBLEMA

En la Actualidad, Transelca S.A. ESP cuenta con una *Gestión Integral de Riesgos* (GIR), "Este manejo tiene como gran objetivo garantizar la continuidad de los negocios de la organización". Las políticas están claramente definidas, pero carecen de herramientas automatizadas que contribuyan a determinar de manera objetiva y oportuna los informes que deben ser presentados a la alta gerencia para la toma de decisiones.

También es importante resaltar, que la *Gestión Integral de Riesgos*, actualmente se encuentra determinada para administrar los riesgos estratégicos de la organización, ésta gestión no abarca la administración de riesgos por procesos y como impactan estos sobre cada recurso empresarial.

Es por ello, que la organización tiene la necesidad de una herramienta automatizada que contribuya a una adecuada gestión y administración de riesgos de manera objetiva, incluyendo la gestión de riesgos por procesos en cada recurso de la organización. **¿Qué aportes significativos se logran con la implementación de una herramienta dinámica para la gestión y administración de riesgos por procesos en Transelca S.A. ESP?**

Con éste proyecto, se pretende dar un enfoque práctico, objetivo y oportuno a la Gestión Integral de Riesgos, buscando que sea aplicado a todos los procesos de la filial Transelca S.A. ESP, logrando de esta forma, tomar las mejores decisiones que conlleven a la expansión de manera segura del grupo, asegurando la continuidad del negocio y disminuyendo pérdidas económicas.

5. GESTIÓN Y ADMINISTRACIÓN DE RIESGOS

5.1 Concepto de riesgos.

Es importante tener muy presente, que siempre existe exposición a riesgos ante cualquier actividad que se realice, determinando así, resultados negativos para la organización.

El riesgo como tal, no es otra cosa que la posibilidad de que un evento desafortunado ocurra, obteniendo de esta materialización un impacto negativo, que puede ir desde pérdidas leves, hasta pérdidas de gran magnitud, como por ejemplo, vidas humanas.

Según la NTC 5254, el riesgo es la posibilidad de que ocurra algo que tendrá impacto sobre los objetivos. Se mide en términos de consecuencia y probabilidad.

5.2 Administración de riegos

En la actualidad, las organizaciones son conscientes que independientemente de su naturaleza, tamaño o razón de ser, están expuestas a diversos riesgos que pueden poner en peligro su existencia, por tal motivo, se hace necesario tener en cuenta todos aquellos hechos o factores que puedan afectar en un momento determinado el cumplimiento de los objetivos institucionales.

Partiendo de allí, se establece el término *administración del riesgo* según la *superintendencia financiera de Colombia,* como: “Conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las entidades vigiladas identifican, miden, controlan y monitorean el riesgo operativo.”

Cabe resaltar que *la administración del riesgo* tiene como fin esencial el manejo y cobertura de los riesgos, para mantener a la organización en dirección de sus objetivos institucionales, promoviendo la eficiencia de las operaciones y mantenimiento del capital.

Por lo anterior, el objetivo es garantizar la solvencia y estabilidad de la empresa, con un manejo adecuado de los riesgos, que permita lograr equilibrio entre la rentabilidad y el riesgo asumido en las operaciones, de tal forma que permita optimizar la relación riesgo-rendimiento[1].

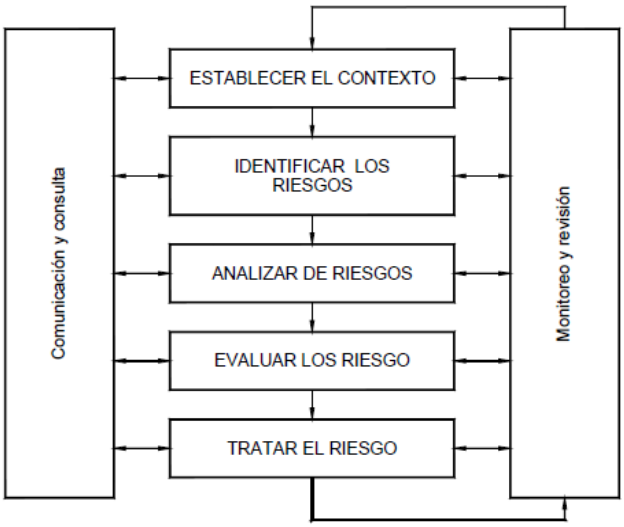
5.2.1 Proceso de administración de riesgos

Es importante precisar, que para determinar una adecuada administración de riesgos, es necesario establecer un completo conjunto de evaluaciones cuantitativas y cualitativas, para tomar las mejores decisiones que ameriten la eficiencia en las diversas operaciones de la organización. El proceso de administración de riesgos está compuesto por una serie de pasos básicos descritos a continuación[2]:

[1] AVILA Bustos, Juan. Medición y control de riesgos financieros en empresas del sector real. Tesis (Contador Público). Bogotá, Colombia, Pontificia Universidad Javeriana, facultad de ciencias económicas, administrativas y contables, 2005, 7 p.

[2] Tomado de Guía para el uso de la norma NTC 5254 gestión del riesgo dentro del proceso de auditoría interna.

Figura 1. Proceso administración del riesgo



Tomado de NTC 5254

5.2.1.1 Establecer el contexto: Establecer el contexto estratégico, organizacional y de gestión del riesgo en el cual ocurrirá el resto del proceso. Es conveniente que se establezcan criterios contra los cuales se va a evaluar el riesgo, y se debe definir la estructura del análisis.

Este requiere establecerse para definir los parámetros básicos dentro de los cuales se debe manejar el riesgo, y para ofrecer orientación con relación a decisiones dentro de estudios de gestión del riesgo más detallados. Aquí se establece el alcance para el resto del proceso de gestión del riesgo.

5.2.1.2 Identificar riesgos: Identificar qué, por qué y cómo pueden surgir elementos como base para análisis posterior.

Es esencial realizar una identificación de conjunto usando un proceso sistemático bien estructurado, debido a que un riesgo potencial no identificado durante esta etapa será excluido del análisis posterior. La identificación debe incluir todos los riesgos, sea que estén o no bajo el control de la organización.

El Decreto 1599 de 2005 lo define como: Elemento de Control, que posibilita conocer los eventos potenciales, estén o no bajo el control de la Entidad Pública, que ponen en riesgo el logro de su Misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia.

La identificación de los riesgos se realiza a nivel del Componente de Direccionamiento Estratégico, identificando los factores internos o externos a la entidad, que pueden ocasionar riesgos que afecten el logro de los objetivos. Es la base del análisis de riesgos que permite avanzar hacia una adecuada implementación de políticas que conduzcan a su control.

5.2.1.3 Analizar riesgos: Determinar los controles existentes y analizar los riesgos en términos de consecuencia y posibilidad en el contexto de estos controles. El análisis debe considerar la gama de consecuencias potenciales y la posibilidad de que éstas ocurran. Se pueden combinar la consecuencia y la posibilidad para producir un nivel estimado de riesgo.

Los objetivos del análisis consisten en separar los riesgos aceptables menores de los mayores, y proporcionar datos que sirvan para la evaluación y el tratamiento de riesgos. El análisis del riesgo incluye considerar las fuentes de riesgo, sus consecuencias y la posibilidad de que estas consecuencias ocurran. Se pueden identificar los factores que afectan las consecuencias y la posibilidad. El riesgo se analiza mediante la combinación de estimaciones de consecuencias y posibilidad en el contexto de las medidas de control existentes.

5.2.1.4 Evaluar los riesgos: Comparar los niveles estimados de riesgo, contra los criterios pre-establecidos. Esto posibilita que los riesgos sean clasificados de modo que se identifiquen prioridades de gestión. Si los niveles de riesgo establecido son bajos, entonces los riesgos pueden encajar en una categoría aceptable, y es posible que no se requiera tratamiento.

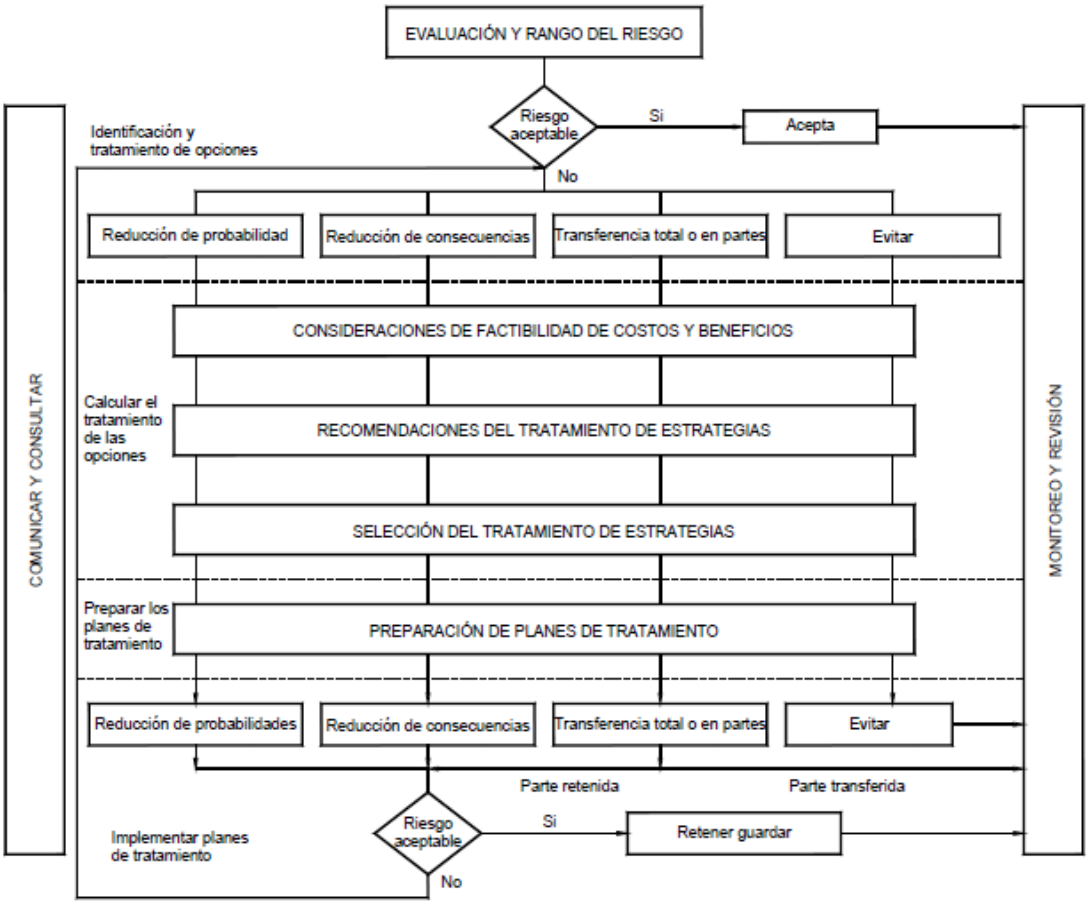
La evaluación del riesgo involucra la comparación del nivel de riesgo encontrado durante el proceso de análisis contra los criterios de riesgo previamente establecidos.

El análisis del riesgo y los criterios contra los cuales se comparan los riesgos en la evaluación del riesgo se deben considerar sobre la misma base. Por tanto, la evaluación cualitativa involucra la comparación de un nivel cualitativo del riesgo contra los criterios cualitativos; y la evaluación cuantitativa involucra la comparación del nivel numérico del riesgo, contra los criterios que pueden expresarse como un número específico, como por ejemplo un valor que indique fatalidad, frecuencia o valor monetario.

5.2.1.5 Tratar los riesgos: Aceptar y monitorear los riesgos de baja prioridad. Para los demás riesgos, desarrollar e implementar un plan de gestión específico que incluya considerar el suministro de recursos.

El tratamiento del riesgo incluye la identificación de la gama de opciones para tratar el riesgo, la evaluación de dichas opciones, la preparación de planes para el tratamiento del riesgo y su implementación.

Figura 2. Tratamiento del riesgo



Tomado de NTC 5254

5.2.1.6Monitorear y revisar: Monitorear y revisar el desempeño del sistema de gestión del riesgo y los cambios que pudieran afectarlo.

Es necesario monitorear los riesgos, la eficacia del plan de tratamiento del riesgo, las estrategias y el sistema de gestión que se establecen para controlar la implementación. Deben monitorearse los riesgos y la eficacia de las medidas de control a fin de garantizar que las circunstancias cambiantes no alteren las prioridades del riesgo. Pocos riesgos permanecen estáticos.

Resulta esencial la revisión permanente para asegurarse de que el plan de gestión continúa sigue siendo pertinente. Los factores que pueden afectar la posibilidad y las consecuencias de un resultado pueden cambiar, al igual que los factores que afectan la conveniencia o el costo de las diferentes opciones de tratamiento. Por consiguiente, es necesario repetir regularmente el ciclo de gestión del riesgo. La revisión es una parte integral del plan de tratamiento de gestión del riesgo.

5.2.1.7 Comunicar y consultar: Comunicar y consultar con las partes interesadas, internas y externas, según sea apropiado, en cada etapa del proceso de gestión del riesgo y con relación al proceso en conjunto.

La comunicación y la consulta constituyen una consideración importante en cada paso del proceso de gestión del riesgo. Resulta primordial desarrollar un plan de comunicación tanto para las partes interesadas internas como para las externas en la etapa más temprana del proceso. Este plan debe tratar asuntos relacionados tanto con el riesgo mismo como con el proceso para gestionarlo.

En éste ítem se incluyen un diálogo bilateral entre las partes interesadas, y los esfuerzos se deben centrar en la consulta, más que en un flujo unilateral de información proveniente de quien toma las decisiones hacia las otras partes interesadas.

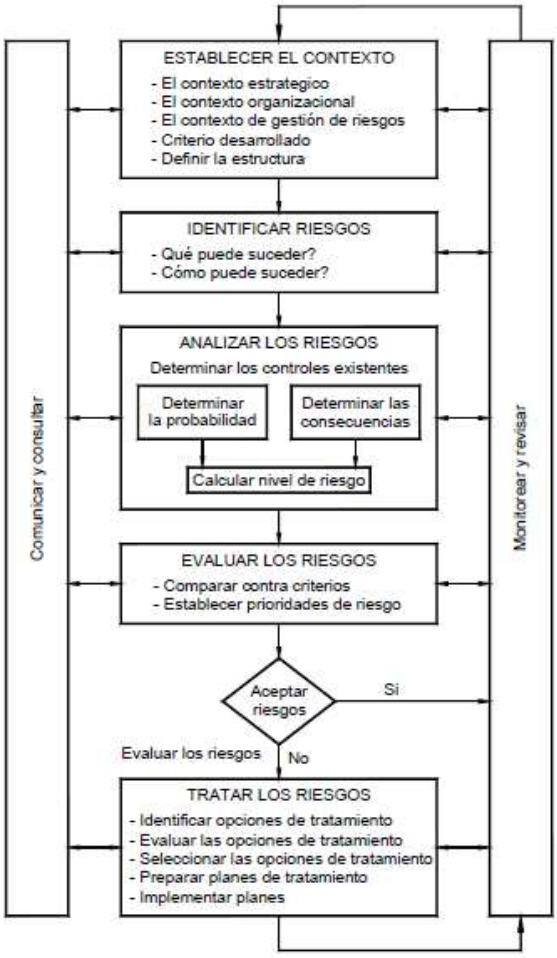
La comunicación interna y externa efectiva es importante para garantizar que quienes son responsables de implementar la gestión del riesgo y quienes tienen un interés creado comprendan la base sobre la cual se toman decisiones y por qué se requieren acciones particulares.

Las percepciones del riesgo pueden variar debido a la diferencia en las creencias, conceptos y las necesidades, asuntos y preocupaciones de las partes interesadas, en la medida en que se relacionan con el riesgo u otros asuntos bajo discusión. Es probable que las partes interesadas realicen juicios acerca de la aceptabilidad de un riesgo con base en su percepción de éste. Puesto que las partes interesadas

pueden tener un impacto significativo en las decisiones tomadas, resulta primordial que se identifiquen y documenten sus percepciones del riesgo, lo mismo que sus percepciones de los beneficios, que se entiendan y traten las razones subyacentes.

Para cada etapa del proceso deben mantenerse registros adecuados que sean suficientes para satisfacer la auditoría independiente.

Figura 3. Proceso completo administración de riesgos



Tomado de NTC 5254

5.3 Clasificación del riesgo

Durante el proceso de identificación del riesgo se recomienda hacer una clasificación de los mismos teniendo en cuenta los siguientes conceptos[3]:

5.3.1 Riesgos Estratégicos: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

5.3.2 Riesgos Operativos: Comprende los riesgos relacionados tanto con la parte operativa como técnica de la entidad, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.

5.3.3 Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluye, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad. De la eficiencia y transparencia en el manejo de los recursos, así como su interacción con las demás áreas dependerá en gran parte el éxito o fracaso de toda entidad.

5.3.4 Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

[3] Tomado de Guía de administración del riesgo, Departamento administrativo de la función pública, República de Colombia

5.3.5 Riesgos de Tecnología: Se asocian con la capacidad de la Entidad para que la tecnología disponible satisfaga las necesidades actuales y futuras de la entidad y soporte el cumplimiento de la misión.

Con la realización de esta etapa se busca que la entidad obtenga los siguientes resultados:

- Determinar las causas (factores internos o externos) de las situaciones identificadas como riesgos para la entidad.
- Describir los riesgos identificados con sus características.
- Precisar los efectos que los riesgos puedan ocasionar a la entidad.

5.4 Factores de riesgo

Se entiende por factores de riesgo, las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operativo[4].

Son factores de riesgo el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.

Dichos factores se deben clasificar en internos o externos, según se indica a continuación.

5.4.1 Factores de riesgo internos

5.4.1.1 Recurso Humano: Es el conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la entidad.

[4] Superintendencia Financiera de Colombia, Circular externa 048 diciembre de 2006: Reglas relativas a la administración del riesgo operativo

Se entiende por vinculación directa, aquella basada en un contrato de trabajo en los términos de la legislación vigente.

La vinculación indirecta hace referencia a aquellas personas que tienen con la entidad una relación jurídica de prestación de servicios diferente a aquella que se origina en un contrato de trabajo.

5.4.1.2 Procesos: Es el conjunto interrelacionado de actividades para la transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad.

5.4.1.3 Tecnología: Es el conjunto de herramientas empleadas para soportar los procesos de la entidad. Incluye: hardware, software y telecomunicaciones.

5.4.1.4 Infraestructura: Es el conjunto de elementos de apoyo para el funcionamiento de una organización. Entre otros se incluyen: edificios, espacios de trabajo, almacenamiento y transporte.

5.4.2 Factores de riesgo Externos

Los factores de riesgo externos, como su nombre lo expresan, son factores que influyen en la organización desde el entorno periférico con el que la entidad interactúa, son factores ajenos y diferentes a toda la gestión que se maneja dentro de la organización, pero, que sin duda alguna, en muchas ocasiones tienen un gran impacto con respecto a los objetivos organizacionales.

Éstos son eventos asociados a la fuerza de la naturaleza u ocasionados por terceros, que escapan en cuanto a su causa y origen al control de la entidad.

5.5 Procedimientos para administrar riesgos[5]

5.5.1 Evitar riesgos: Un riesgo es evitado cuando en la organización no se acepta. Esta técnica puede ser más negativa que positiva. Si el evitar riesgos fuera usado excesivamente el negocio sería privado de muchas oportunidades de ganancia *(por ejemplo: arriesgarse a hacer una inversión)* y probablemente no alcanzaría sus objetivos.

5.5.2 Reducir riesgos: Los riegos pueden ser reducidos, por ejemplo con: programas de seguridad, guardias de seguridad, alarmas y estimación de futuras pérdidas con la asesoría de personas expertas.

5.5.3 Aceptar riesgos: Es quizás el más común de los métodos para enfrentar los riesgos, pues muchas veces una acción positiva no es transferirlo o reducir su acción. Cada organización debe decidir cuales riegos se retienen, o se transfieren basándose en su margen de contingencia, una pérdida puede ser un desastre financiero para organización siendo fácilmente sostenido por otra organización.

5.5.4 Compartir riesgos: Cuando los riesgos son compartidos, la posibilidad de pérdida es transferida del individuo al grupo.

5.6 Políticas de administración del riesgo[6]

La organización define y documenta la política para administración de riesgos, incluyendo los objetivos y su compromiso con la administración de riesgos. La política de administración de riesgos debe ser relevante para el contexto estratégico de la organización y para las metas, objetivos y naturaleza del

[5] Tomado de: http://www.gestiopolis.com/recursos/documentos/fulldocs/ger1/sistecinfor.htm

[6] GUTIERREZ Correa, Juan. Sistematización del proceso de gestión integral de riesgos para una empresa administradora del mercado de energía colombiano, Tesis (ingeniero de sistemas y computación). Pereira, Colombia, Universidad Tecnológica de Pereira, facultad de ingenierías, 2008, 18 p.

negocio. La gerencia asegurará que ésta política es comprendida, implementada y mantenida en todos los niveles de la organización

6. CONTROL INTERNO ORGANIZACIONAL

6.1 Concepto de Control interno.

El concepto de control interno, el cual es tan relevante para el auditor interno como externo, ha ido evolucionando a lo largo del tiempo. La idea general del control forma parte de la teoría de la Administración, está en el manejo o gobierno de hechos, cosas y en la dirección de todos los individuos. Antes de dar una definición de Control Interno es conveniente definir por separado que se entiende por Control y que se entiende por Interno.

- Control, implica revisar, fiscalizar. Para efectuar control es necesario predeterminar objetivos, pues sin objetivo el control no tiene sentido.
- Interno, es algo situado dentro de los límites de un negocio o entidad.

La evaluación del sistema de Control Interno es también necesaria para la labor de los auditores internos y externos. La confianza en los controles internos nos permite definir el alcance, oportunidad, naturaleza y profundidad de las pruebas.

6.2 Definición de Control Interno según COSO

El informe COSO (*Committee of Sponsoring Organizations*), define el Control Interno como “un proceso efectuado por la dirección y el resto de integrantes de una organización, destinado a proveer una razonable seguridad en el logro de los objetivos:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes y reglamentaciones.

Mientras que los directivos fijan pautas de lineamientos y definen la filosofía directiva, los Auditores internos y externos brindan asesoramiento en la evaluación del sistema de control interno. Por tanto el personal de la organización debe tener claro su papel dentro del sistema y a la importancia de los controles.

También podemos decir que el Control Interno está dirigido a ayudar a la gerencia en el cumplimiento de los objetivos y metas organizacionales. Para que un sistema de control interno sea eficaz es necesario implementar procesos reguladores de evaluación que permitan adaptarlo a los cambios o necesidades del mercado. Podemos decir, entonces que, el Control Interno es un proceso no es un hecho aislado, sino una serie de acciones estrechamente relacionadas con las actividades de la organización; los procesos relacionados son: Planificación, Ejecución y Supervisión y por tanto serán más efectivos si se construyen dentro de una infraestructura.

Cabe resaltar que el factor humano es vital en todo este proceso, ya que son las personas quienes planifican y realizan las actividades, controlan que los objetivos organizacionales se cumplan. Es la propia dirección quien sentara las bases de un ambiente de control adecuado, definirá los valores éticos, los códigos de conducta, contribuyendo así a crear la cultura organizacional deseada.

Es importante mencionar que ningún sistema de control interno puede proporcionar una seguridad absoluta en el cumplimiento de los objetivos. Existen ciertas limitaciones inherentes al sistema y están relacionadas con los siguientes elementos:

- Error humano o fallas: errores debido a malos entendidos, distracciones, fatiga por cambios del personal en los procesos de reestructura o por el simple hecho del error humano.

- Abuso de autoridad por parte de altos ejecutivos o directivos: la dirección actúa en contra de los procedimientos establecidos con fines ilegítimos o en provecho propio, tal es el caso de la información o documentación falsa.
- Colusión: dos o más personas se ponen de acuerdo para cometer fraude violando los controles establecidos.
- Costo-beneficio: como los recursos materiales y humanos son escasos a la hora de implementar los controles las organizaciones deben considerar la relación costo-beneficio.
- Actividades repetitivas: generalmente los controles se implantan para las actividades repetitivas, pero cuando ocurren situaciones imprevistas, extraordinarias, existe la posibilidad de que el sistema de control interno no responda efectivamente.

La eficacia o no de un sistema de control interno va a depender de la subjetividad del evaluador y de la percepción de los 5 componentes del sistema según COSO[7]:

- Ambiente de control
- Apreciación del riesgo
- Actividades de control
- Información y comunicación
- Monitoreo

[7]The Institutes of Internal Auditors Research Foundation (IIARF), Evaluación eficaz del sistema de control interno. 1 ed, Florida, 2008. 21 p. ISBN 978-0-89413-621-4

6.3 Componentes de Control Interno Según COSO

El informe COSO define al control interno como una pirámide compuesta de cinco componentes interrelacionados que forman parte del proceso de gestión. Los componentes del control interno son:

- Ambiente de control
- Apreciación del riesgo
- Actividades de control
- Información y comunicación
- Monitoreo

6.3.1. Ambiente de Control

Sirve de base para el resto de componentes del sistema y ejerce influencia relevante en cada uno de los demás componentes. Establece el tono de una organización y la conciencia de control de su gente.

Por otro lado también podemos decir que el ambiente de control se define como el conjunto de circunstancias que enmarcan el accionar de una entidad desde la perspectiva del control interno y que son por lo tanto determinantes del grado en que los principios de este último imperan sobre las conductas y los procedimientos organizacionales.

Es, fundamentalmente, consecuencia de la actitud asumida por la alta dirección, la gerencia, y por carácter reflejo, los demás agentes con relación a la importancia del control interno y su incidencia sobre las actividades y resultados, fija el tono de la organización y, sobre todo, provee disciplina a través de la influencia que ejerce sobre el comportamiento del personal en su conjunto.

Constituye el andamiaje para el desarrollo de las acciones y de allí deviene su trascendencia, pues como conjunción de medios, operadores y reglas previamente definidas, traduce la influencia colectiva de varios factores en el establecimiento,

fortalecimiento o debilitamiento de políticas y procedimientos efectivos en una organización.

Los principales factores del ambiente de control son[8]:

- La filosofía y estilo de la dirección y la gerencia.
- La estructura, el plan organizacional, los reglamentos y los manuales de procedimiento.
- La integridad, los valores éticos, la competencia profesional y el compromiso de todos los componentes de la organización, así como su adhesión a las políticas y objetivos establecidos.
- Las formas de asignación de responsabilidades y de administración y desarrollo del personal.
- El grado de documentación de políticas y decisiones, y de formulación de programas que contengan metas, objetivos e indicadores de rendimiento.
- En las organizaciones que lo justifiquen, la existencia de consejos de administración y comités de auditoría con suficiente grado de independencia y calificación profesional.

El ambiente de control reinante será tan bueno, regular o malo como lo sean los factores que lo determinan. El mayor o menor grado de desarrollo y excelencia de éstos hará, en ese mismo orden, a la fortaleza o debilidad del ambiente que generan y consecuentemente al tono de la organización.

[8]Tomado de: http://www.sigen.gov.ar/documentacion/ngcind.asp

6.3.2. Apreciación del Riesgo[9]

Es la evaluación cualitativa y cuantitativa de la exposición al riesgo en las diferentes actividades o procesos. El rol primario de la gerencia es colocar los activos a riesgo para alcanzar los objetivos:

- Humanos,
- Físicos,
- Financieros,
- Intangibles.

El rol primario del auditor interno es evaluar e informar sobre los controles gerenciales los cuales aseguran que los objetivos establecidos para eficiencia y eficacia son cumplidos. Los recursos son eficientemente usados, y las necesidades de los clientes están siendo debidamente cubiertas.

La apreciación de los riesgos del negocio comienza con el planeamiento estratégico y el riesgo de cambios en el entorno. La apreciación de riesgos intenta analizar los riesgos en las unidades operativas a través de la cadena de valor. Un planeamiento estructurado es un efectivo sistema de control interno. A través del planeamiento, los gerentes anticipan los riesgos inherentes en sus actividades y toman métodos para mitigar los efectos de dichos riesgos. Riesgos inherentes, también son denominados riesgos del negocio, y existen en todas las actividades. El riesgo inherente de cualquier actividad es una función de un mix de activos y la naturaleza de la actividad.

6.3.2.1 Diferentes estadios en la apreciación de riesgos

Apreciación de los riesgos del negocio significa la apreciación de riesgos y oportunidades que afectan el desarrollo de las metas y objetivos de la organización. Los riesgos pueden ser apreciados en tres niveles:

[9] Tomado de: http://www.ccee.edu.uy/ensenian/catcoint/material/riesgos.PDF

- Estratégico: Esta apreciación de riesgos se utiliza como guía de la organización durante un prolongado período de tiempo (hasta diez años). Dicho procedimiento es usualmente realizado por la Dirección y Alta Gerencia:
- Proceso / programa / procesos: Esta apreciación de riesgos es utilizada, desarrollada y gerenciada durante el período actual de la organización. El gerente del proceso, programa o proceso es la persona que inicialmente tiene la responsabilidad de la apreciación.
- Operacional: Utilizado en las operaciones diarias. Esta apreciación es usualmente realizada por el nivel de supervisión o por individuos o equipos de trabajos designados para tal tarea.

6.3.3 Actividades de Control

Las actividades de control son las políticas y los procedimientos que ayudan a asegurar que se lleven a cabo las instrucciones de la dirección de la empresa. Ayudan a asegurar que se tomen las medidas necesarias para controlar los riesgos relacionados con la consecución de los objetivos de la empresa. Hay actividades de control en toda la organización, a todos los niveles y en todas las funciones.

“Deben establecerse y ajustarse políticas y procedimientos que ayuden a conseguir una seguridad razonable de que se llevan a cabo en forma eficaz las acciones consideradas necesarias para afrontar los riesgos que existen respecto a la consecución de los objetivos de la unidad”.

Las actividades de control existen a través de toda la organización y se dan en toda la organización, a todos los niveles y en todas las funciones, e incluyen cosas tales como; aprobaciones, autorizaciones, verificaciones, conciliaciones, análisis de la eficacia operativa, seguridad de los activos, y segregación de funciones. En algunos entornos, las actividades de control se clasifican en; controles

preventivos, controles de detección, controles correctivos, controles manuales o de usuario, controles informáticos o de tecnología de información, y controles de la dirección. Independientemente de la clasificación que se adopte, las actividades de control deben ser adecuadas para los riesgos.
Hay muchas posibilidades diferentes en lo relativo a actividades concretas de control, lo importante es que se combinen para formar una estructura coherente de control global

Las empresas pueden llegar a padecer un exceso de controles hasta el punto que las actividades de control les impidan operar de manera eficiente, lo que disminuye la calidad del sistema de control. Por ejemplo, un proceso de aprobación que requiera firmas diferentes puede no ser tan eficaz como un proceso que requiera una o dos firmas autorizadas de funcionarios componentes que realmente verifiquen lo que están aprobando antes de estampar su firma. Un gran número de actividades de control o de personas que participan en ellas no asegura necesariamente la calidad del sistema de control.

6.3.4. Información y Comunicación

Se debe identificar, recopilar y comunicar información pertinente en forma y plazo que permitan cumplir a cada empleado con sus responsabilidades. Los sistemas informáticos producen informes que contienen información operativa, financiera y datos sobre el cumplimiento de las normas que permite dirigir y controlar el negocio de forma adecuada. Dichos sistemas no sólo manejan datos generados internamente, sino también información sobre acontecimientos internos, actividades y condiciones relevantes para la toma de decisiones de gestión así como para la presentación de información a terceros. También debe haber una comunicación eficaz en un sentido más amplio, que fluya en todas las direcciones a través de todos los ámbitos de la organización, de arriba hacia abajo y a la inversa.

Todo el personal, especialmente el que cumple importantes funciones operativas o financieras, debe recibir y entender el mensaje de la alta dirección, de que las obligaciones en materia de control deben tomare en serio. Asimismo debe conocer su propio papel en el sistema de control interno, así como la forma en que sus actividades individuales se relacionan con el trabajo de los demás. Si no se conoce el sistema de control, los cometidos específicos y las obligaciones en el sistema, es probable que surjan problemas. Los empleados también deben conocer cómo sus actividades se relacionan con el trabajo de los demás.

Debe existir una comunicación efectiva a través de toda la organización. El libre flujo de ideas y el intercambio de información son vitales. La comunicación en sentido ascendente es con frecuencia la más difícil, especialmente en las organizaciones grandes. Sin embargo, es evidente la importancia que tiene.

El fomentar un ambiente adecuado para promover una comunicación abierta y efectiva está fuera del alcance de los manuales de políticas y procedimientos. Depende del ambiente que reina en la organización y del tono que da la alta dirección. Además de la comunicación interna debe existir una comunicación efectiva con entidades externas tales como accionistas, autoridades, proveedores y clientes. Ello contribuye a que las entidades correspondientes comprendan lo que ocurre dentro de la organización y se mantengan bien informadas. Por otra parte, la información comunicada por entidades externas a menudo contiene datos importantes sobre el sistema de control interno.

6.3.5. Monitoreo o Supervisión[10]

Los sistemas de control interno requieren supervisión, es decir, un proceso que comprueba que se mantiene el adecuado funcionamiento del sistema a lo largo del tiempo. Esto se consigue mediante actividades de supervisión continuada, evaluaciones periódicas o una combinación de ambas cosas.

[10] Tomado de: http://www.degerencia.com/articulo/los_cinco_componentes_del_control_interno

La supervisión continuada se da en el transcurso de las operaciones. Incluye tanto las actividades normales de dirección y supervisión, como otras actividades llevadas a cabo por el personal en la realización de sus funciones. El alcance y la frecuencia de las evaluaciones periódicas dependerán esencialmente de una evaluación de los riesgos y de la eficacia de los procesos de supervisión continuada.

Las deficiencias detectadas en el control interno deberán ser notificadas a niveles superiores, mientras que la alta dirección y el consejo de administración deberán ser informados de los aspectos significativos observados. "Todo el proceso debe ser supervisado, introduciéndose las modificaciones pertinentes cuando se estime necesario. De esta forma el sistema puede reaccionar ágilmente y cambiar de acuerdo a las circunstancias".

Es preciso supervisar continuamente los controles internos para asegurarse de que el proceso funciona según lo previsto. Esto es muy importante porque a medida que cambian los factores internos y externos, controles que una vez resultaron idóneos y efectivos pueden dejar de ser adecuados y de dar a la dirección la razonable seguridad que ofrecían antes.

El alcance y frecuencia de las actividades de supervisión dependen de los riesgos a controlar y del grado de confianza que inspira a la dirección el proceso de control. La supervisión de los controles internos puede realizarse mediante actividades continuas incorporadas a los procesos empresariales y mediante evaluaciones separadas por parte de la dirección, de la función de auditoría interna o de personas independientes. Las actividades de supervisión continua destinadas a comprobar la eficacia de los controles internos incluyen las actividades periódicas de dirección y supervisión, comparaciones, conciliaciones, y otras acciones de rutina.

Luego del análisis de cada uno de los componentes, podemos sintetizar que éstos, vinculados entre sí:

- Generan una sinergia y forman un sistema integrado que responde de una manera dinámica a las circunstancias cambiantes del entorno.
- Son influidos e influyen en los métodos y estilos de dirección aplicables en las empresas e inciden directamente en el sistema de gestión, teniendo como premisa que el hombre es el activo más importante de toda organización y necesita tener una participación más activa en el proceso de dirección y sentirse parte integrante del Sistema de Control Interno que se aplique.
- Están entrelazados con las actividades operativas de la entidad coadyuvando a la eficiencia y eficacia de las mismas.
- Permiten mantener el control sobre todas las actividades.
- Su funcionamiento eficaz proporciona un grado de seguridad razonable de que una o más de las categorías de objetivos establecidas van a cumplirse. Por consiguiente, estos componentes también son criterios para determinar si el control interno es eficaz.
- Marcan una diferencia con el enfoque tradicional de control interno dirigido al área financiera.
- Coadyuvan al cumplimiento de los objetivos organizacionales en sentido general

6.4. Tipos de Controles.

Estos son usados para definir cualquier actividad o acción realizada manualmente y/o automáticamente y así detectar, prevenir y corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos.

6.4.1. Controles Preventivos

Un control interno que se usa para prevenir eventos indeseables, errores u otras ocurrencias que pudieran tener un efecto material negativo sobre un proceso o producto final, de acuerdo a la organización. [COBIT: 2006], también trata de evitar accesos a software no autorizados

6.4.2. Controles Detectivos[11]

Cuando fallan los preventivos para tratar de conocer cuanto antes el evento, en otras palabras Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los más importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos

6.4.3. Controles Correctivos[12]

Facilitan la vuelta a la normalidad cuándo se han producido incidencias, también nos ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en sí, es una actividad altamente propensa a errores.

6.5. ISO/IEC 27002:2005 Tabla de Controles

Este Estándar Internacional va orientado a la seguridad de la información en las empresas u organizaciones, de modo que las probabilidades de ser afectados por robo, daño o pérdida de información se minimicen al máximo.

[11] Tomado de: http://es.scribd.com/doc/61220171/12/b-CONTROLES-DETECTIVOS
[12] Tomado de: http://es.scribd.com/doc/61220171/12/b-CONTROLES-CORRECTIVOS

Figura 4. Lista de controles ISO 27000

ISO/IEC 27002:2005. Dominios (11), Objetivos de control (39) y Controles (133)

CLIC SOBRE CADA CONTROL PARA MÁS INFORMACIÓN

Versión actualizada de esta lista en: http://www.iso27000.es/download/ControlesISO27002-2005.pdf

5. POLÍTICA DE SEGURIDAD.
5.1 Política de seguridad de la información.
5.1.1 Documento de política de seguridad de la información.
5.1.2 Revisión de la política de seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Compromiso de la Dirección con la seguridad de la información.
6.1.2 Coordinación de la seguridad de la información.
6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.
6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
6.1.5 Acuerdos de confidencialidad.
6.1.6 Contacto con las autoridades.
6.1.7 Contacto con grupos de especial interés.
6.1.8 Revisión independiente de la seguridad de la información.
6.2 Terceros.
6.2.1 Identificación de los riesgos derivados del acceso de terceros.
6.2.2 Tratamiento de la seguridad en la relación con los clientes.
6.2.3 Tratamiento de la seguridad en contratos con terceros.
7. GESTIÓN DE ACTIVOS.
7.1 Responsabilidad sobre los activos.
7.1.1 Inventario de activos.
7.1.2 Propiedad de los activos.
7.1.3 Uso aceptable de los activos.
7.2 Clasificación de la información.
7.2.1 Directrices de clasificación.
7.2.2 Etiquetado y manipulado de la información.
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
8.1 Antes del empleo.
8.1.1 Funciones y responsabilidades.
8.1.2 Investigación de antecedentes.
8.1.3 Términos y condiciones de contratación.
8.2 Durante el empleo.
8.2.1 Responsabilidades de la Dirección.
8.2.2 Concienciación, formación y capacitación en seg. de la informac.
8.2.3 Proceso disciplinario.
8.3 Cese del empleo o cambio de puesto de trabajo.
8.3.1 Responsabilidad del cese o cambio.
8.3.2 Devolución de activos.
8.3.3 Retirada de los derechos de acceso.
9. SEGURIDAD FÍSICA Y DEL ENTORNO.
9.1 Áreas seguras.
9.1.1 Perímetro de seguridad física.
9.1.2 Controles físicos de entrada.
9.1.3 Seguridad de oficinas, despachos e instalaciones.
9.1.4 Protección contra las amenazas externas y de origen ambiental.
9.1.5 Trabajo en áreas seguras.
9.1.6 Áreas de acceso público y de carga y descarga.
9.2 Seguridad de los equipos.
9.2.1 Emplazamiento y protección de equipos.
9.2.2 Instalaciones de suministro.
9.2.3 Seguridad del cableado.
9.2.4 Mantenimiento de los equipos.
9.2.5 Seguridad de los equipos fuera de las instalaciones.
9.2.6 Reutilización o retirada segura de equipos.
9.2.7 Retirada de materiales propiedad de la empresa.
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.
10.1 Responsabilidades y procedimientos de operación.
10.1.1 Documentación de los procedimientos de operación.
10.1.2 Gestión de cambios.
10.1.3 Segregación de tareas.
10.1.4 Separación de los recursos de desarrollo, prueba y operación.
10.2 Gestión de la provisión de servicios por terceros.
10.2.1 Provisión de servicios.
10.2.2 Supervisión y revisión de los servicios prestados por terceros.
10.2.3 Gestión del cambio en los servicios prestados por terceros.
10.3 Planificación y aceptación del sistema.
10.3.1 Gestión de capacidades.
10.3.2 Aceptación del sistema.
10.4 Protección contra el código malicioso y descargable.
10.4.1 Controles contra el código malicioso.
10.4.2 Controles contra el código descargado en el cliente.
10.5 Copias de seguridad.
10.5.1 Copias de seguridad de la información.
10.6 Gestión de la seguridad de las redes.
10.6.1 Controles de red.
10.6.2 Seguridad de los servicios de red.
10.7 Manipulación de los soportes.
10.7.1 Gestión de soportes extraíbles.
10.7.2 Retirada de soportes.
10.7.3 Procedimientos de manipulación de la información.
10.7.4 Seguridad de la documentación del sistema.
10.8 Intercambio de información.
10.8.1 Políticas y procedimientos de intercambio de información.
10.8.2 Acuerdos de intercambio.
10.8.3 Soportes físicos en tránsito.
10.8.4 Mensajería electrónica.
10.8.5 Sistemas de información empresariales.
10.9 Servicios de comercio electrónico.
10.9.1 Comercio electrónico.
10.9.2 Transacciones en línea.
10.9.3 Información públicamente disponible.
10.10 Supervisión.
10.10.1 Registros de auditoría.
10.10.2 Supervisión del uso del sistema.
10.10.3 Protección de la información de los registros.
10.10.4 Registros de administración y operación.
10.10.5 Registro de fallos.
10.10.6 Sincronización del reloj.
11. CONTROL DE ACCESO.
11.1 Requisitos de negocio para el control de acceso.
11.1.1 Política de control de acceso.
11.2 Gestión de acceso de usuario.
11.2.1 Registro de usuario.
11.2.2 Gestión de privilegios.
11.2.3 Gestión de contraseñas de usuario.
11.2.4 Revisión de los derechos de acceso de usuario.
11.3 Responsabilidades de usuario.
11.3.1 Uso de contraseñas.
11.3.2 Equipo de usuario desatendido.
11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
11.4 Control de acceso a la red.
11.4.1 Política de uso de los servicios en red.
11.4.2 Autenticación de usuario para conexiones externas.
11.4.3 Identificación de los equipos en las redes.
11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
11.4.5 Segregación de las redes.
11.4.6 Control de la conexión a la red.
11.4.7 Control de encaminamiento (routing) de red.
11.5 Control de acceso al sistema operativo.
11.5.1 Procedimientos seguros de inicio de sesión.
11.5.2 Identificación y autenticación de usuario.
11.5.3 Sistema de gestión de contraseñas.
11.5.4 Uso de los recursos del sistema.
11.5.5 Desconexión automática de sesión.
11.5.6 Limitación del tiempo de conexión.
11.6 Control de acceso a las aplicaciones y a la información.
11.6.1 Restricción del acceso a la información.
11.6.2 Aislamiento de sistemas sensibles.
11.7 Ordenadores portátiles y teletrabajo.
11.7.1 Ordenadores portátiles y comunicaciones móviles.
11.7.2 Teletrabajo.
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.
12.1 Requisitos de seguridad de los sistemas de información.
12.1.1 Análisis y especificación de los requisitos de seguridad.
12.2 Tratamiento correcto de las aplicaciones.
12.2.1 Validación de los datos de entrada.
12.2.2 Control del procesamiento interno.
12.2.3 Integridad de los mensajes.
12.2.4 Validación de los datos de salida.
12.3 Controles criptográficos.
12.3.1 Política de uso de los controles criptográficos.
12.3.2 Gestión de claves.
12.4 Seguridad de los archivos de sistema.
12.4.1 Control del software en explotación.
12.4.2 Protección de los datos de prueba del sistema.
12.4.3 Control de acceso al código fuente de los programas.
12.5 Seguridad en los procesos de desarrollo y soporte.
12.5.1 Procedimientos de control de cambios.
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
12.5.3 Restricciones a los cambios en los paquetes de software.
12.5.4 Fugas de información.
12.5.5 Externalización del desarrollo de software.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Control de las vulnerabilidades técnicas.
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
13.1 Notificación de eventos y puntos débiles de seguridad de la información.
13.1.1 Notificación de los eventos de seguridad de la información.
13.1.2 Notificación de puntos débiles de seguridad.
13.2 Gestión de incidentes y mejoras de seguridad de la información.
13.2.1 Responsabilidades y procedimientos.
13.2.2 Aprendizaje de los incidentes de seguridad de la información.
13.2.3 Recopilación de evidencias.
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
14.1.2 Continuidad del negocio y evaluación de riesgos.
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
14.1.4 Marco de referencia para la planificación de la cont. del negocio.
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.
15. CUMPLIMIENTO.
15.1 Cumplimiento de los requisitos legales.
15.1.1 Identificación de la legislación aplicable.
15.1.2 Derechos de propiedad intelectual (DPI).
15.1.3 Protección de los documentos de la organización.
15.1.4 Protección de datos y privacidad de la información de carácter personal.
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
15.1.6 Regulación de los controles criptográficos.
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.
15.2.1 Cumplimiento de las políticas y normas de seguridad.
15.2.2 Comprobación del cumplimiento técnico.
15.3 Consideraciones sobre las auditorías de los sistem. de información.
15.3.1 Controles de auditoría de los sistemas de información.
15.3.2 Protección de las herramientas de auditoría de los sist. de inform.

Documento sólo para uso didáctico. La norma oficial debe adquirirse en entidades autorizadas para su venta

Ver. 4.0, 16-1-2011

Tomada de: http://www.iso27000.es/download/ControlesISO27002-2005.pdf

7. Antecedentes de la Empresa Transelca S.A. E.S.P.

7.1. Misión

Brindar servicios de transporte de energía y conexión al sistema eléctrico en los mercados nacional e internacional, con altos criterios de eficiencia y eficacia en un ambiente de mejoramiento continuo que satisfaga las necesidades y expectativas de nuestros grupos de interés, de acuerdo con las políticas del Grupo Empresarial ISA.

7.2. Visión

TRANSELCA contribuirá, en el año 2016, a la MEGA del Grupo Empresarial con ingresos de 135 millones de dólares, logrando a su vez:

- Ser reconocida en Colombia como líder en el negocio de las conexiones al Sistema Interconectado Nacional.
- Liderar la explotación de los negocios de Conexión del mercado en Centro América y el Caribe.

7.3. Valores Corporativos

- **Ética:** Carácter moral de nuestros actos en tanto estén encaminados hacia el bien individual o colectivo. Un pensamiento ético genera actitudes y acciones transparentes.
- **Responsabilidad Social**: Compromiso con la búsqueda de una mejor calidad de vida para sus empleados, sus familias, el medio ambiente y la sociedad en general.
- **Innovacion**: Introducción de aspectos nuevos en la organización y en el servicio que contribuyan al logro de los objetivos.

- **Excelencia:** Cumplimiento con los estándares de calidad en la prestación de los servicios que lleve a un reconocimiento diferenciador frente a los competidores.

7.3.1. Valores Diferenciadores

- **Liderazgo:** Identificación y apoyo al potencial de los trabajadores para trabajar en equipo y convocar a los miembros de la organización en el desarrollo de proyectos y cumplimiento de los objetivos y compromisos de la empresa.
- **Seguridad:** Protección de los trabajadores y contratistas, la información, los equipos y los bienes, a través de la identificación y entendimiento de los riesgos inherentes a nuestro negocio y su administración.
- **Respeto:** Es la esencia de las relaciones humanas de la vida en comunidad, del trabajo en equipo, de la vida conyugal. El respeto es la garantía absoluta de transparencia, integridad y seriedad. Exige cumplimiento y permite crear un ambiente de cordialidad y conciliación

7.4. Políticas

7.4.1. Política de control interno (GRUPO EMPRESARIAL ISA) Aprobada en Junta Directiva No. 654 del 27 de julio de 2007

Con esta política el Grupo ISA declara sus criterios, y marco de actuación respecto al control interno, como parte de los mecanismos de direccionamiento y control que facilitan la búsqueda de unidad de propósito y dirección.

7.4.2. Política de gestión humana: Somos un Grupo Empresarial en el que bajo los principios de Unidad de Propósito y Dirección propiciamos el crecimiento de nuestro Talento Humano, conscientes de su importancia para el logro de la competitividad.

La Política de Gestión Humana del **Grupo Empresarial ISA**, establece el compromiso recíproco entre cada una de las Empresas del Grupo y sus respectivos trabajadores de crear un ambiente laboral que propicie el desarrollo integral del personal en los aspectos: humano, laboral y social, sobre la base de construir identidad con el Direccionamiento Estratégico del Grupo: Visión, misión, objetivos y estrategia corporativa.

Esta política contribuye efectivamente a atraer, desarrollar y retener el talento humano que cada una de las Empresas del Grupo necesita para desarrollar su gestión, ser competitiva, alcanzar su visión y lograr el Desarrollo Integral Compartido: Hombre – Organización.

7.4.3. Política de inversión: Con esta política el Grupo Empresarial ISA, en la búsqueda de la unidad de propósito y dirección, declara los criterios y define el marco de actuación dentro de los cuales se realizará el análisis y evaluación, toma de decisión y seguimiento de las inversiones, buscando que aseguren el crecimiento con rentabilidad del Grupo Empresarial y permitan la generación de valor

7.4.4. Política de servicio: Con la política de servicio todas las empresas del Grupo ISA hacen explícito el compromiso y definen un marco general de actuación para ofrecer a sus clientes productos y servicios de calidad y construir relaciones de largo plazo.

En cada una de las empresas del Grupo ISA, como parte de su estrategia, se busca satisfacer los clientes mediante organizaciones eficientes para conocerlos, interpretarlos y servirlos integralmente.

El contenido de la Política de Servicio enmarca el pensamiento institucional y los lineamientos generales de todas las empresas del Grupo ISA, de tal forma que se

pueda dar cumplimiento a las normas y estándares de calidad, tanto en los ámbitos específicos de cada país como en el ámbito internacional.

7.4.5. Política social: La Política Social del Grupo ISA establece el marco de referencia para la actuación de sus empresas respecto a las sociedades en las cuales tienen presencia, considerando sus formas organizativas, expresiones culturales, situación socioeconómica y niveles territoriales. Como resultado de una gestión social responsable, las empresas del Grupo ISA esperan ser reconocidas como organizaciones legítimas, confiables y comprometidas con el desarrollo sostenible de la sociedad.

7.4.6. Política de comunicación: Aprobada en Junta Directiva No. 654 del 27 de julio de 2007

La Política de Comunicación responde al proceso de construcción de una identidad corporativa como Grupo Empresarial y a la necesidad de establecer un marco de referencia que facilite la gestión empresarial y las relaciones entre las Empresas del Grupo, así como la interacción y el diálogo con el entorno.

Con esta política el Grupo ISA adopta un enfoque estratégico de la comunicación, en el sentido de comprometerse con un desarrollo coherente de los procesos de comunicación y el reconocimiento a los diferentes interlocutores como parte de un sistema de relaciones.

7.4.7. Política de salud ocupacional: Aprobada en Junta Directiva No. 651 del 27 de abril de 2007

Con esta política el Grupo ISA declara su compromiso de proteger, mantener y mejorar la salud ocupacional de sus trabajadores y de las personas que intervienen en la ejecución de sus procesos.

7.4.8. Política para la gestión integral de riesgos: Con esta política el Grupo ISA declara sus criterios y define el marco de actuación para la gestión integral de los riesgos que generan vulnerabilidad en los recursos empresariales, requeridos en todos los procesos que son críticos para la continuidad y competitividad de las empresas que conforman el Grupo.

7.4.9. Política ambiental: Aprobada en Junta Directiva No. 651 del 27 de abril de 2007

Con esta política, el Grupo ISA declara su compromiso con la gestión ambiental, aplicable a todas sus operaciones empresariales.

7.4.10. Política de información y del conocimiento: Con esta política, las empresas del Grupo ISA declaran los criterios y definen el marco de actuación para la gestión de la información y del conocimiento como activos estratégicos de la organización.

Al promulgar esta política, las empresas del Grupo ISA reafirman:

- Su convicción de que la información y el conocimiento tienen un valor estratégico, en consecuencia son protegidos, administrados y potencializados como activos intangibles
- Su compromiso con el respeto a la propiedad intelectual en los términos definidos por la ley.
- Su compromiso y alcance con los diferentes grupos de interés respecto al acceso y suministro de información que maneja la organización en desarrollo de sus actividades
- La importancia de la información y el conocimiento para construir sinergias entre las empresas del Grupo.
- Su enfoque hacia la promoción y desarrollo de una cultura de seguridad de información.

7.4.11. Política de adquisición de bienes y servicios: Aprobada en Junta Directiva No. 660 del 14 de diciembre de 2007

Con esta Política todas las empresas del Grupo ISA homologan principios y conceptos relacionados con la adquisición de bienes y servicios y hacen explícitos sus compromisos con los proveedores.

7.4.11.1 Marco de referencia jurídico: Las empresas del Grupo ISA acatan, respetan y aplican la normatividad en materia de contratación vigente en cada uno de los países donde se encuentren localizadas. Así mismo aplican todos los convenios, acuerdos y tratados bilaterales y multilaterales que resulten pertinentes. El Grupo ISA se compromete a respetar los acuerdos que tenga con los accionistas minoritarios.

7.4.11.2 Marco de referencia conceptual

- **Normatividad interna:** Instrumentos por los cuales la Junta Directiva, Directorio o su equivalente, adopta un reglamento para la contratación de bienes y servicios en cada una de las empresas del Grupo.
- **Negociación:** Proceso de interacción potencialmente beneficioso, por el que dos o más partes buscan una concertación de intereses a través de acciones decididas conjuntamente.

7.4.11.3 Alcance de la política: Las empresas del Grupo ISA desarrollarán procesos de adquisición de bienes y servicios ágiles, oportunos, eficientes y con reglas claras, que proporcionen economías de escala y aseguren la competitividad, respetando los criterios de buena fe, transparencia y economía.

7.4.11.4 Criterios de aplicación:

- **Buena Fe:** Es el obrar debido, leal, honesto y ético, que deben observar las partes durante las etapas pre-contractual, contractual y post-contractual, y

en consecuencia, los contratos obligarán no sólo a lo pactado expresamente en ellos, sino a todo lo que corresponda a la naturaleza de los mismos, según la ley de tal manera que se genere entre las partes confianza, credibilidad y seguridad.

- **Transparencia:** Los procesos de adquisición deben realizarse con base en procedimientos claros, imparciales y objetivos que garanticen la igualdad de condiciones y oportunidades de los proponentes.
- **Economía:** Los procesos de adquisición se adelantarán de tal manera que las empresas del Grupo puedan seleccionar la propuesta que convenga a sus intereses y ejecutar el contrato respectivo haciendo la mejor inversión en recursos técnicos, económicos y humanos.

7.4.11.5 Marco de actuación: Las empresas del Grupo ISA:

- Buscan sinergias y economías de escala para el Grupo, cuando sea conveniente y posible.
- Expiden, a través de sus Asambleas o Juntas de socios, Juntas Directivas, Directorios o equivalentes, normatividad interna según sus necesidades particulares, acatando esta política y la legislación vigente en cada país.
- Cuentan con una metodología de negociación de acuerdo con esta política.
- Buscan el mejoramiento continúo de los procesos de adquisición de bienes y servicios con el fin de lograr los mejores resultados en sus negocios.
- Acatan la Política para la Gestión Integral de Riesgos en lo relacionado con los análisis necesarios para preservar la integridad de los recursos empresariales y aplican las metodologías propuestas.
- Contratan bienes y servicios con empresas que aseguren el cumplimiento de las especificaciones y requisitos de las Políticas de Salud Ocupacional y Ambiental del Grupo y que cuenten con mecanismos para garantizar la seguridad de las personas que trabajan para los proveedores.
- Los trabajadores de las empresas del Grupo ISA:

- Se comprometen a vigilar la correcta ejecución de la adquisición de bienes y servicios y a proteger los derechos de la empresa, respondiendo por sus actuaciones y omisiones o el incumplimiento de sus deberes legales y obligaciones asignadas por la empresa.

7.5. Reseña histórica

TRANSELCA como parte del grupo empresarial ISA es una empresa de servicios públicos mixta, constituida como sociedad anónima, que presta servicios de transporte de energía eléctrica en alta tensión y ofrece al mercado servicios de conexión al Sistema de Interconectado Nacional, Administración, Operación y Mantenimiento -AOM- de activos eléctricos y otros asociados a su negocio fundamental.

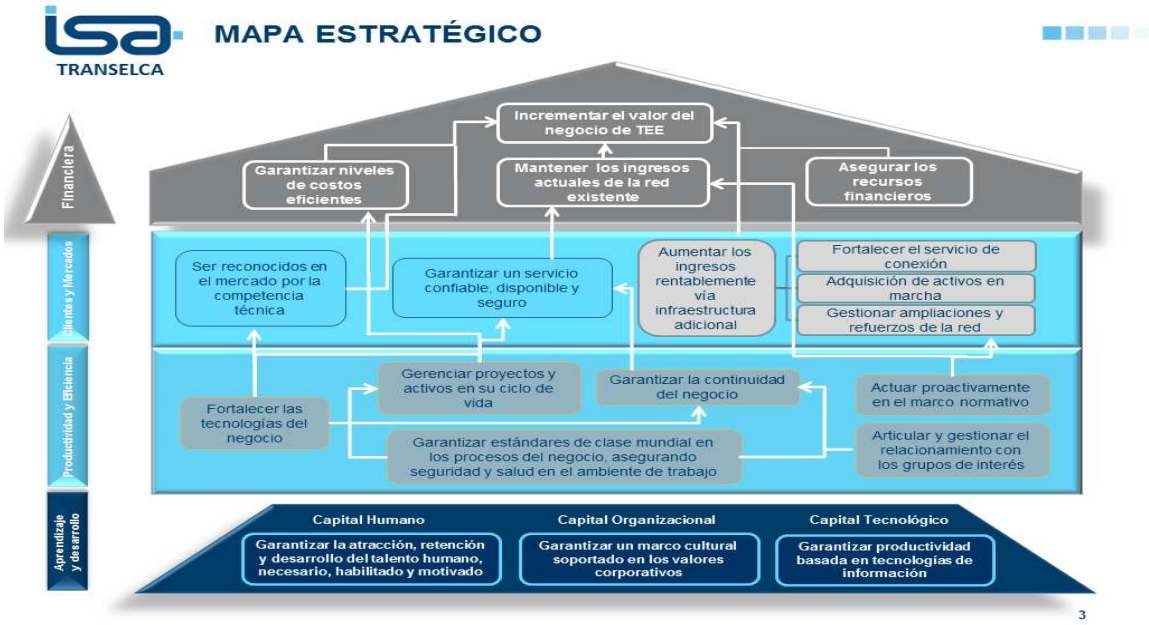
7.6. Estrategia Competitiva

Acorde con el direccionamiento estratégico del Grupo ISA, TRANSELCA enfoca su estrategia competitiva en la Generación de Valor para sus Grupos de Interés, en especial para los accionistas.

En este sentido formula su visión, misión y despliega la estrategia definiendo sus objetivos estratégicos bajo cuatro perspectivas: Financiera, Clientes y Mercados, Productividad y Eficiencia y Aprendizaje y Desarrollo Organizacional.
Estos objetivos se plasman en un mapa estratégico, para luego identificar los indicadores y las metas que serán el mecanismo para evaluar el cumplimiento de la estrategia formulada.

A continuación se presenta el mapa estratégico:

Figura 5. Mapa estratégico Grupo ISA, Transelca S.A. ESP



Tomada de: Grupo ISA, TRANSELCA S.A. ESP. Mapa estratégico

7.7. El Negocio

TRANSELCA a marzo de 2012 tiene una participación del 10.31% en el Sistema de Transmisión Nacional, constituyéndose en la segunda entre las 11 empresas de transmisión del país. Para la prestación de sus servicios, TRANSELCA utiliza una infraestructura eléctrica de su propiedad conformada por 1.532 km de línea de transmisión a 220 kV, 13,75 km de línea de transmisión a 110 y 34.5 kV y una capacidad de transformación de 3.143 MVA en diez (10) subestaciones a 220 kV, dos (2) a 110 kV y una (1) a 34,5 kV. Además cuenta con un Centro de Control dotado con tecnología de punta, que permite atender con calidad y confiabilidad la supervisión de su infraestructura eléctrica, facilitando el cumplimiento de los requerimientos y necesidades de sus clientes.

7.8. Proyección internacional

Por séptimo año consecutivo TRANSELCA recibió calificación "AAA" (Triple A) por parte de la calificadora de riesgos Duff&Phelps de Colombia S.A. para las emisiones de bonos de deuda pública interna. Su excelente calificación de riesgo le ha facilitado su expansión en el sector eléctrico latinoamericano con una participación accionaría del 54.86% en Interconexión Eléctrica ISA Perú S.A, 30% en Red de Energía del Perú y 48,99% en ISA Bolivia.

7.9. Gestión Integral de Riesgos (GIR)

Es la implementación sistemática de un conjunto de acciones tendientes al manejo óptimo de los riesgos en todos los procesos. "Este manejo tiene como gran objetivo garantizar la continuidad de los negocios de la organización".

El ciclo de la Gestión Integral de Riesgos tiene como punto de partida el mapa estratégico corporativo y competitivo del grupo empresarial. Este Ciclo comprende: IDENTIFICACIÓN, EVALUACIÓN, MANEJO, MONITOREO, COMUNICACIÓN Y DIVULGACIÓN EN TODAS LAS ETAPAS.

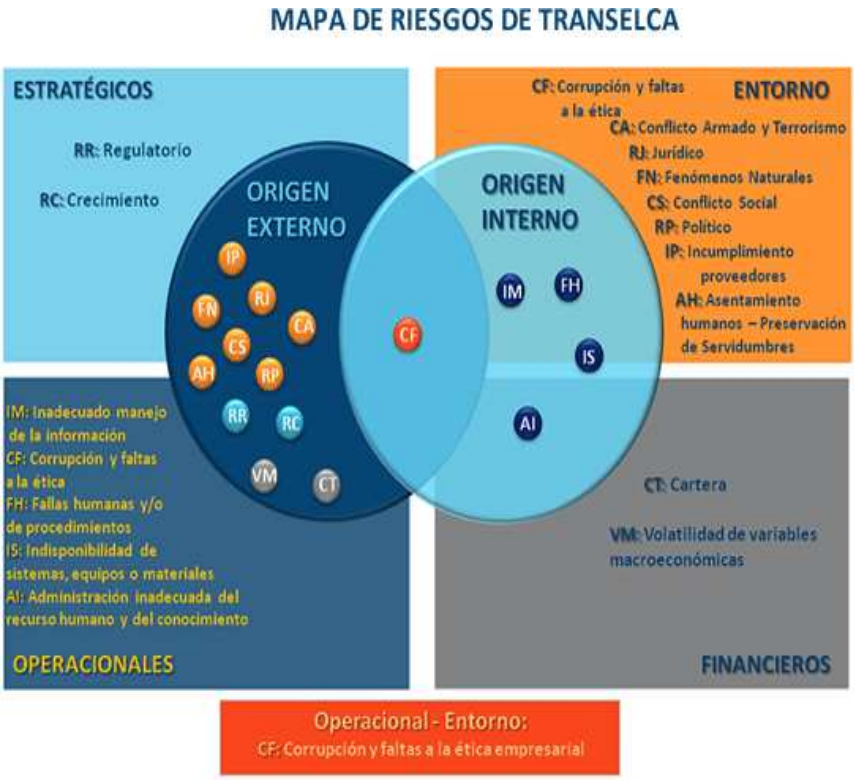
7.10. Ciclo de la Gestión Integral de Riesgos

Figura 6. Gestión integral de riesgos

Tomada de: Grupo ISA, Transelca S.A. ESP

7.11. Mapa de riesgos Transelca S.A.ESP

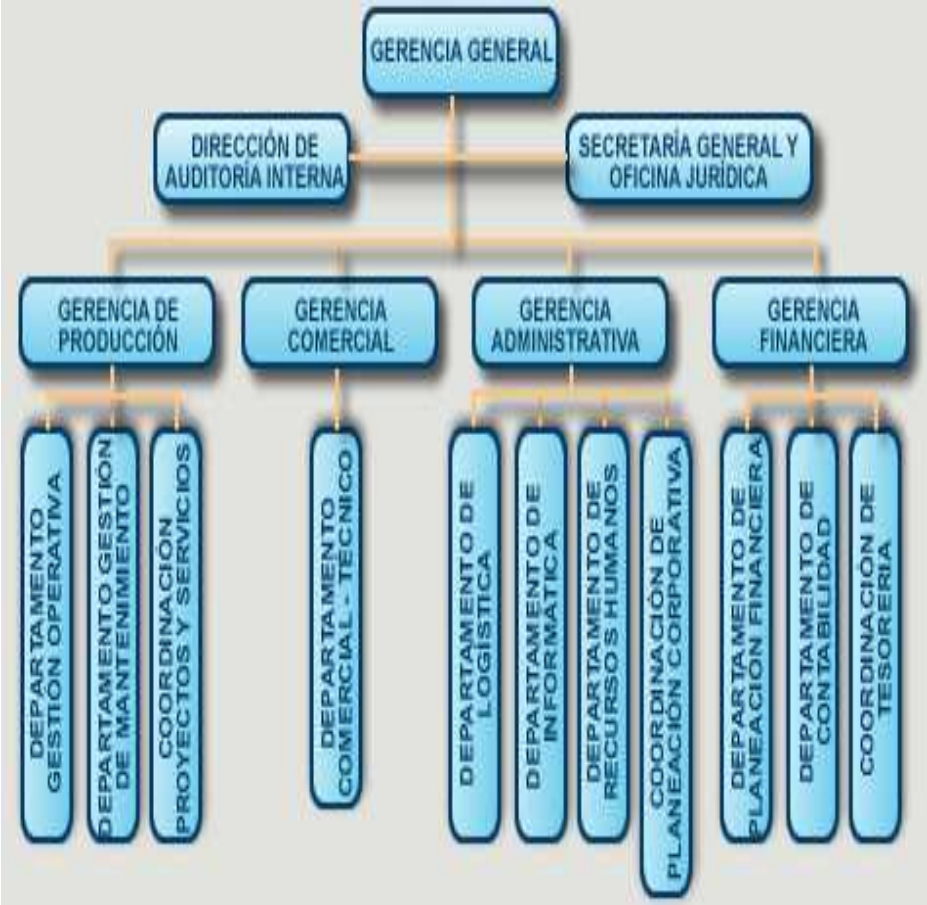
Figura 7. Mapa de riesgos Transelca



Tomada de: Grupo ISA, Transelca S.A. ESP

7.12. Organigrama

Figura 8. Organigrama Transelca S.A. ESP.



Tomado de: Grupo ISA, Transelca S.A. ESP

8. DISEÑO E IMPLEMENTACIÓN DE HERRAMIENTA DINÁMICA APLICADA AL PROCESO DE ADQUISICIÓN DE BIENES Y/O SERVICIOS DE TRANSELCA S.A. E.S.P.

8.1 Diseño de matriz para la descripción y análisis de riesgos

Al momento de diseñar la matriz de administración de riesgos de Transelca S.AESP, se tuvo muy presente los antecedentes manejados por la organización en cuanto a la administración de riesgos estratégicos, se mantuvo criterios antes establecidos, que fueron adaptados de acuerdo con normas vigentes como la NTC 5254.

Para el diseño de ésta matriz, se establece el proceso, luego el subproceso asociado al respectivo proceso, seguidamente los riesgos inherentes asociados al proceso o subproceso, a partir de allí, la descripción del riesgo, clasificación generalizada del riesgo y las implicaciones que estos puedan tener sobre la organización.

Dentro de la matriz, se establece el "control de proceso", a través del ciclo PHVA (Planear, Hacer, Verificar, Actuar) compuesto por las cuatro fases básicas del control: planificar, ejecutar, verificar y actuar correctivamente[13]. Es importante resaltar que las fases del control se enfocan en la parte correctiva, en el diseño que se plantea en éste proyecto, se enfoca de manera preventiva como primera instancia.

[13] Tomado de: http://www.unalmed.edu.co/josemaya/Ing_prod/Control%20de%20Proceso-%20Metodo.pdf

Tabla 1. Primera parte de la matriz gestión y administración de riesgos

PROCESO	SUBPROCESO	RIESGO	CLASIFICACIÓN DEL RIESGO	IMPLICACIONES	ETAPAS PHVA

Tabla creada por autores.

Para la siguiente fase de la matriz, determinar el riesgo puro y residual por recurso, se realiza teniendo en cuenta los recursos homologados por el Grupo Empresarial:

- Recurso Financiero
- Recurso Humano
- Recurso Imagen corporativa
- Recurso Información

Dentro de estos recursos se establecen escalas de probabilidad y severidad para evaluar el riesgo puro de la siguiente forma:

Tabla 2. Escala de severidad

ESCALA DE SEVERIDAD	
Nivel	**Valor relativo**
1	Leve
2	Moderado
3	Crítico
4	Muy Crítico

Tabla 3. Escala de probabilidad

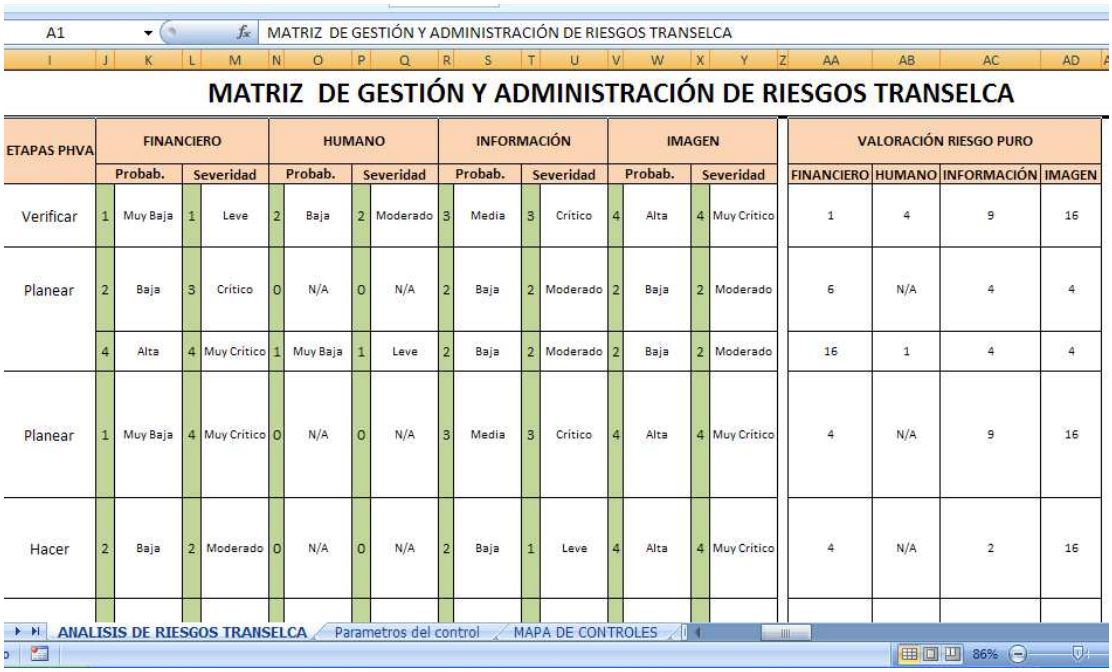
ESCALA DE PROBABILIDAD	
Nivel	**Valor relativo**
1	Muy Baja
2	Baja
3	Media
4	Alta

Tomadas de: Grupo ISA, Transelca S.A. ESP

Es importante resaltar, que en caso de que un riesgo, no aplique a uno o varios recursos, éste será marcado como (N/A) y cuyo valor será marcado con cero (0).

Al momento de establecer el riesgo puro, se multiplica la probabilidad de ocurrencia del evento por la severidad o impacto que dicho evento llegase a ocasionar, en caso de que se materializara; quedando la matriz de la siguiente forma:

Figura 9. Recursos homologados por Transelca S.A ESP y riesgo puro



MATRIZ DE GESTIÓN Y ADMINISTRACIÓN DE RIESGOS TRANSELCA

ETAPAS PHVA	FINANCIERO				HUMANO				INFORMACIÓN				IMAGEN				VALORACIÓN RIESGO PURO			
	Probab.		Severidad		Probab.		Severidad		Probab.		Severidad		Probab.		Severidad		FINANCIERO	HUMANO	INFORMACIÓN	IMAGEN
Verificar	1	Muy Baja	1	Leve	2	Baja	2	Moderado	3	Media	3	Critico	4	Alta	4	Muy Critico	1	4	9	16
Planear	2	Baja	3	Critico	0	N/A	0	N/A	2	Baja	2	Moderado	2	Baja	2	Moderado	6	N/A	4	4
	4	Alta	4	Muy Critico	1	Muy Baja	1	Leve	2	Baja	2	Moderado	2	Baja	2	Moderado	16	1	4	4
Planear	1	Muy Baja	4	Muy Critico	0	N/A	0	N/A	3	Media	3	Critico	4	Alta	4	Muy Critico	4	N/A	9	16
Hacer	2	Baja	2	Moderado	0	N/A	0	N/A	2	Baja	1	Leve	4	Alta	4	Muy Critico	4	N/A	2	16

Imagen creada por autores.

La siguiente parte de la matriz gestión y administración del riesgo, es la que incluye el tratamiento a seguir, la medida de administración aplicada, la ejecución del respectivo control y el riesgo residual.

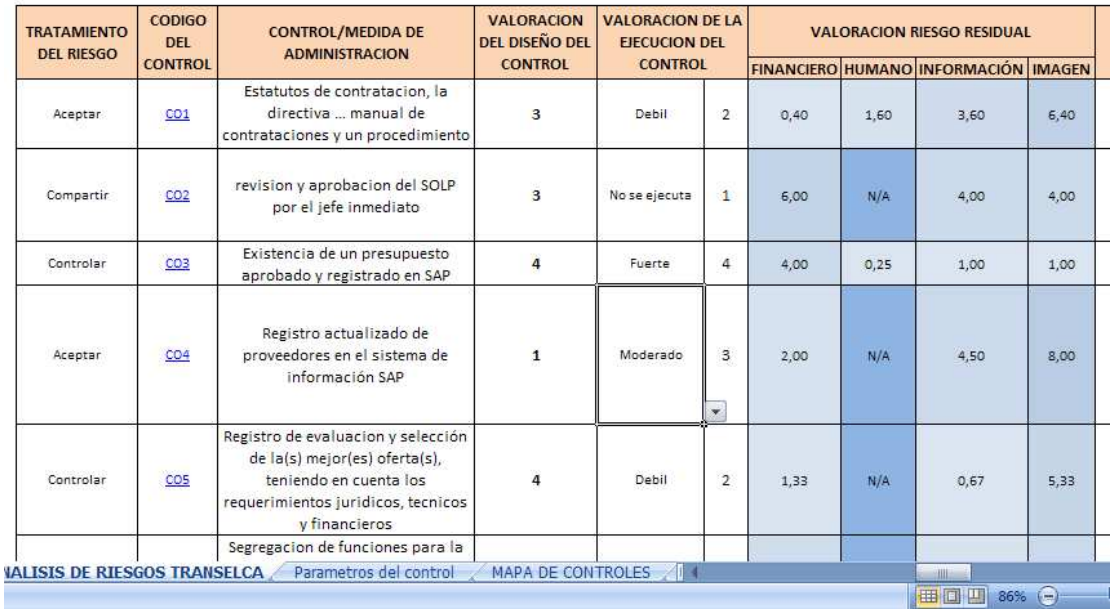
Para ello, se establece los diferentes tratamientos, según los lineamientos manejados por Transelca S.A. ESP en la administración de riesgos estratégicos, que pueden ser: aceptar, compartir y/o controlar el riesgo, en ésta matriz, el otro tratamiento sugerido es evitar, no se incluye porque es obvio que los procesos y riesgos sobre los que se trabaja son controlados; puesto que se trabaja con procesos en ejecución.

Por otra parte, encontramos el código del control, el control o medida de administración, la valoración del diseño del control y la valoración de la ejecución del control, estos tres últimos ítems mencionados tienen que ver con las medidas adoptadas por la organización para mitigar el riesgo, el diseño del control se determina mediante la aplicación que será explicada más adelante.

Retomando ésta parte de la matriz, aquí encontramos el riesgo residual, siendo éste, el resultado de los riesgos puros o inherentes a los procesos tratados con medidas de administración, en la matriz se representa como el riesgo puro, dividido entre el promedio del diseño del control con la ejecución del control, en la eventualidad que exista un adecuado diseño del control, pero dicho control no se ejecuta, el resultado del riesgo residual será igual al riesgo puro.

De ésta manera, tercera parte de la matriz, queda de la siguiente forma:

Figura 10. Medidas de administración y riesgo residual.



TRATAMIENTO DEL RIESGO	CODIGO DEL CONTROL	CONTROL/MEDIDA DE ADMINISTRACION	VALORACION DEL DISEÑO DEL CONTROL	VALORACION DE LA EJECUCION DEL CONTROL		VALORACION RIESGO RESIDUAL			
						FINANCIERO	HUMANO	INFORMACIÓN	IMAGEN
Aceptar	CO1	Estatutos de contratacion, la directiva ... manual de contrataciones y un procedimiento	3	Debil	2	0,40	1,60	3,60	6,40
Compartir	CO2	revision y aprobacion del SOLP por el jefe inmediato	3	No se ejecuta	1	6,00	N/A	4,00	4,00
Controlar	CO3	Existencia de un presupuesto aprobado y registrado en SAP	4	Fuerte	4	4,00	0,25	1,00	1,00
Aceptar	CO4	Registro actualizado de proveedores en el sistema de información SAP	1	Moderado	3	2,00	N/A	4,50	8,00
Controlar	CO5	Registro de evaluacion y selección de la(s) mejor(es) oferta(s), teniendo en cuenta los requerimientos juridicos, tecnicos y financieros	4	Debil	2	1,33	N/A	0,67	5,33
		Segregacion de funciones para la							

Imagen creada por autores.

8.2 Diseño de matriz para establecer parámetros de control

Con el diseño de la matriz de parámetros de control, se buscaba una mayor objetividad, puesto que actualmente la calificación que se da al diseño de un control es muy subjetiva y depende de personal altamente calificado en la materia. Teniendo en cuenta que cada persona expone sus razones o punto de vista, en ésta matriz se busco diferentes valores ponderados entre diferentes expertos y personal que manejan el tema de medidas de administración dentro de Transelca S.A. ESP, llegando a un punto común y tratando de dar valores cuantitativos, para determinar de la manera más objetiva posible, los valores del diseño del control.

Para determinar en primera instancia los valores que puede tomar el diseño de un control, se ponderaron los siguientes valores así:

- **Tipo de control:** Se define como la oportunidad de acción ante el riesgo que se pretende mitigar, normalmente, se sugieren tres tipos de control:

-Preventivo: Controles claves que actúan sobre los riesgos de cada proceso, antes de que se materialicen, se califica con 100 puntos.

-Detectivo: Controles que actúan sobre los riesgos una vez se han detectado, se califica con 50 puntos.

-Correctivo: Controles que actúan sobre los riesgos para corregir la materialización del riesgo, se califica con 20 puntos.

En éste proyecto se sugiere un tipo de control, llamado control de Protección, sugerido por el Dr. Jairo Salazar, quien explica que es un control que actúa como hibrido entre el control preventivo y detectivo, este control se califica con 80 puntos.

La ponderación para éste ítem es de un 15%.

- **Clase de control:** Se define como la clasificación del control en cuanto al mecanismo de acción, se clasifica de la siguiente forma:

  -Automático: si es ejecutado de manera automatizada por un sistema previamente programado, se califica con 100 puntos.

  -Semiautomático: por una persona que controla el sistema que ejecuta el control, se califica con 50 puntos.

  -Manual: es ejecutado un control totalmente por una persona sin ayudas tecnológicas, se califica con 20 puntos.

  La ponderación para éste ítem es de un 15%.

- **Redundancia:** La idea es determinar qué alternativas ofrece el control con respecto a la mitigación de un riesgo, se determina las siguiente posibilidades:

  - Redundante y agrega valor: Este ítem determina que tan robusto puede ser un control y que otra alternativa de protección puede ofrecer un control, que sin generar un costo adicional, puede ofrecer una doble protección, se califica con 100 puntos.

- No redundante y agrega valor: Es un control que ofrece una sola alternativa, pero es tan robusta, que con ella existe una protección adecuada, se califica con 80 puntos.
- Redundante y no agrega valor: Es un control que ofrece diversos pasos que son realizados por la naturaleza del control, pero no aportan ninguna protección extra, se califica con 0 puntos.
-No redundante y no agrega valor: Es un control que ofrece una sola alternativa, pero no ofrece ninguna protección, se califica con 0 puntos.

La ponderación del ítem es de 7%.

- **Frecuencia:** La frecuencia con que se ejecutaría el control, se determina de la siguiente forma:

  -Permanente: El control siempre estará activo, se califica con 100 puntos, se califica con 100 puntos.

  -Periódico: El control se ejecutaría pasado un periodo determinado de tiempo, se califica con 100 puntos.

  -Ocasional: El control se ejecutara por momentos aleatorios durante la ejecución del proceso, se califica con 100 puntos.

  -Sin definir: El control esta, pero no se especifican tiempos de ejecución, se califica con 0 puntos.

  La ponderación del ítem es de 10%.

- **Adecuada naturaleza del control:** La adecuada naturaleza del control, determina la precisión con que éste fue diseñado específicamente para mitigar un determinado riesgo, o tan solo es un control que mitiga un riesgo en un bajo porcentaje, pero que no fue establecido para ese tipo de riesgo, si la naturaleza del control para mitigar un riesgo es adecuada, se califica con 100 puntos, si es inadecuada con 0 puntos.

  Éste ítem se pondera con un 15%.

- **Normalizado:** Se refiere a la documentación dentro de las normas requeridas, normalizado son 100 puntos, no normalizado 0 puntos.
  La ponderación de éste ítem es de 7%.

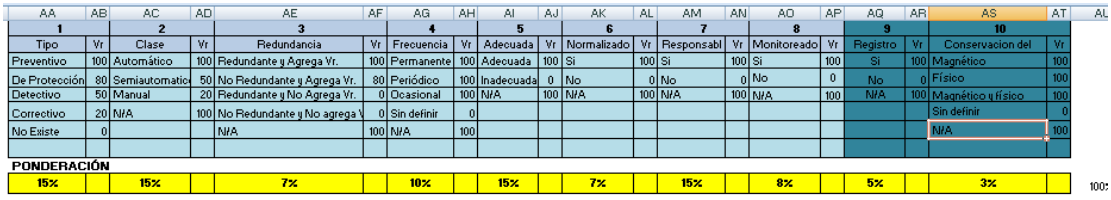
- **Responsable:** Se refiere a la asignación de un funcionario que se enmarque como responsable del control, 100 puntos si tiene responsable, 0 puntos si no existe.
  La ponderación de éste ítem es de 15%.

- **Monitoreado:** Es importante que un control se revise periódicamente a fin de determinar si cumple con la función de mitigar el riesgo, si ésta monitoreado se le dan 100 puntos, de lo contrario 0 puntos.
  La ponderación de éste ítem es de 8%.

- **Registro:** Un control puede dejar huellas, por llamarlo así de alguna forma, si un control mantiene un adecuado registro, recibe 100 puntos, de lo contrario 0 puntos.
  La ponderación para éste ítem es de 5%.

- **Conservación del registro:** Lo ideal para hacerle seguimiento a un control, es revisar los registros que éste dejaría, éstos podrían ser magnéticos, físicos, o magnéticos y físicos; lo importante como tal, es poder monitorear también, a través de dichos registros. Para tal caso, el hecho de que un control mantenga un adecuado registro, amerita 100 puntos en afán de cuantificar el diseño del control.
  La ponderación para éste ítem es de 3%.

Figura 11. Valores ponderados diseño del control.



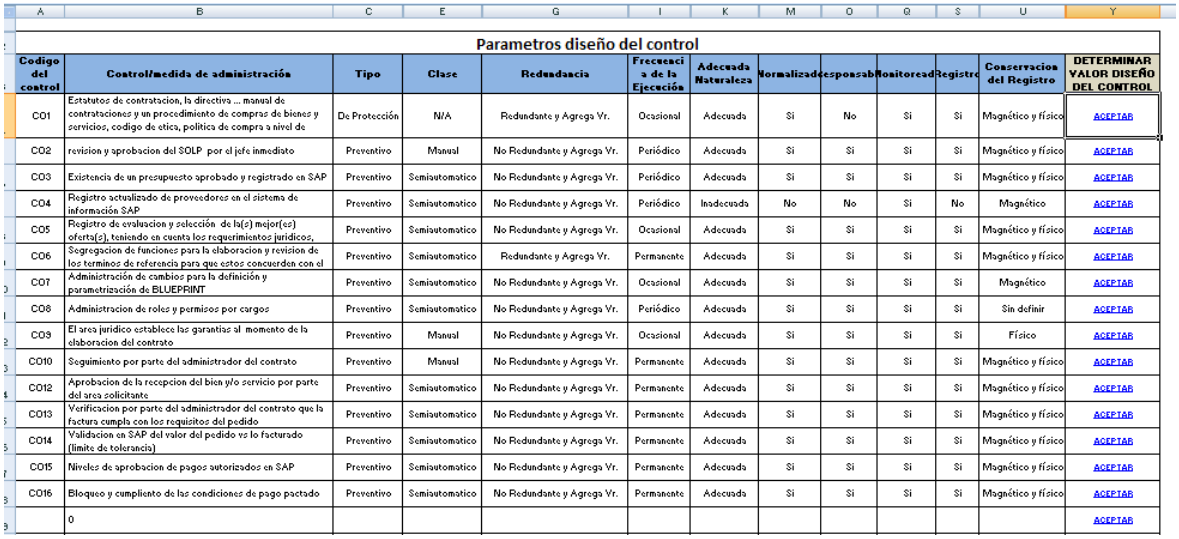
AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AL
1		2		3		4		5		6		7		8		9		10		
Tipo	Vr	Clase	Vr	Redundancia	Vr	Frecuencia	Vr	Adecuada	Vr	Normalizado	Vr	Responsabl	Vr	Monitoreado	Vr	Registro	Vr	Conservacion del	Vr	
Preventivo	100	Automático	100	Redundante y Agrega Vr.	100	Permanente	100	Adecuada	100	Si	100	Si	100	Si	100	Si	100	Magnético	100	
De Protección	80	Semiautomatico	50	No Redundante y Agrega Vr.	80	Periódico	100	Inadecuada	0	No	0	No	0	No	0	No	0	Físico	100	
Detectivo	50	Manual	20	Redundante y No Agrega Vr.	0	Ocasional	100	N/A	100	N/A	100	N/A	100	N/A	100	N/A	100	Magnético y físico	100	
Correctivo	20	N/A	100	No Redundante y No agrega V	0	Sin definir	0											Sin definir	0	
No Existe	0			N/A	100	N/A	100											N/A	100	
PONDERACIÓN																				
15%		15%		7%		10%		15%		7%		15%		8%		5%		3%		100

Imagen creada por autores,

Por otra parte, una vez establecidos los criterios para determinar la ponderación, seguimos con la matriz diseño del control, la cual consta de los valores antes mencionados, relacionándola con la matriz análisis de riesgos, mediante el código del control, el nombre del control.

Para volver a la matriz análisis de riesgos y de paso calcular el valor del diseño del control, nos vamos a la columna determinar valor diseño del control, se le da aceptar al control que se está evaluando, obteniendo así un valor cuantitativo, muy objetivo del diseño del control, el cual se verá reflejado en la matriz antes mencionada, con un valor que luego será promediado con la ejecución del control, para de esta forma determinar el riesgo residual.

Figura 12. Matriz parámetros diseño del control



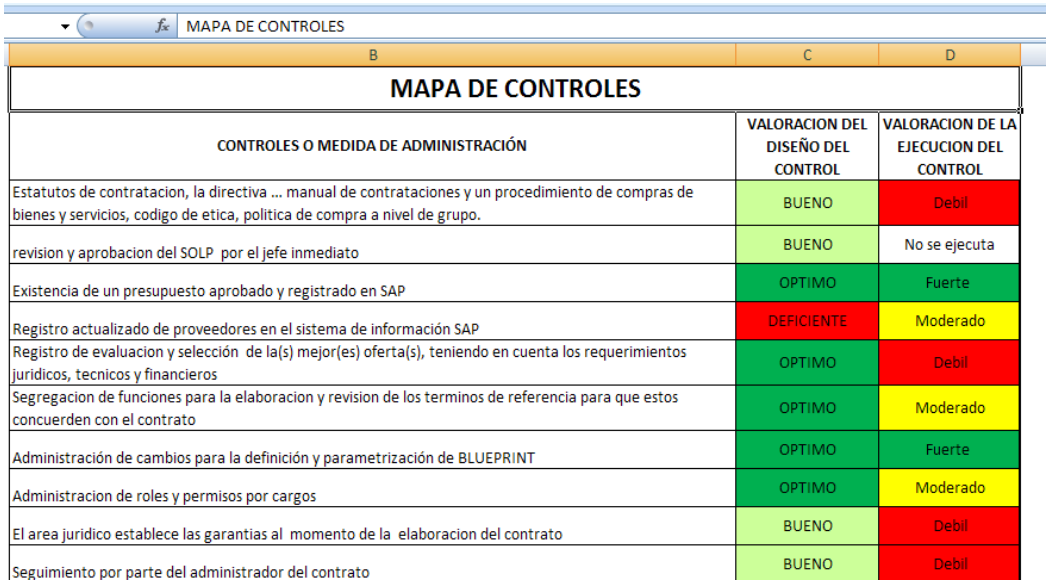
Parametros diseño del control												
Codigo del control	Control/medida de administración	Tipo	Clase	Redundancia	Frecuencia de la Ejecución	Adecuada Naturaleza	Normalizada	esponsab	Monitorea	Registro	Conservacion del Registro	DETERMINAR VALOR DISEÑO DEL CONTROL
CO1	Estatutos de contratacion, la directiva ... manual de contrataciones y un procedimiento de compras de bienes y servicios, codigo de etica, politica de compra a nivel de	De Protección	N/A	Redundante y Agrega Vr.	Ocasional	Adecuada	Si	No	Si	Si	Magnético y físico	ACEPTAR
CO2	revision y aprobacion del SOLP por el jefe inmediato	Preventivo	Manual	No Redundante y Agrega Vr.	Periódico	Adecuada	Si	Si	Si	Si	Magnético y físico	ACEPTAR
CO3	Existencia de un presupuesto aprobado y registrado en SAP	Preventivo	Semiautomatico	No Redundante y Agrega Vr.	Periódico	Adecuada	Si	Si	Si	Si	Magnético y físico	ACEPTAR
CO4	Registro actualizado de proveedores en el sistema de información SAP	Preventivo	Semiautomatico	No Redundante y Agrega Vr.	Periódico	Inadecuada	No	No	Si	No	Magnético	ACEPTAR
CO5	Registro de evaluacion y selección de la(s) mejor(es) oferta(s), teniendo en cuenta los requerimientos juridicos,	Preventivo	Semiautomatico	No Redundante y Agrega Vr.	Ocasional	Adecuada	Si	Si	Si	Si	Magnético y físico	ACEPTAR
CO6	Segregacion de funciones para la elaboracion y revision de los terminos de referencia para que estos concuerden con el	Preventivo	Semiautomatico	Redundante y Agrega Vr.	Permanente	Adecuada	Si	Si	Si	Si	Magnético y físico	ACEPTAR
CO7	Administración de cambios para la definición y parametrización de BLUEPRINT	Preventivo	Semiautomatico	No Redundante y Agrega Vr.	Ocasional	Adecuada	Si	Si	Si	Si	Magnético	ACEPTAR
CO8	Administracion de roles y permisos por cargos	Preventivo	Semiautomatico	No Redundante y Agrega Vr.	Periódico	Adecuada	Si	Si	Si	Si	Sin definir	ACEPTAR
CO9	El area juridico establece las garantias al momento de la elaboracion del contrato	Preventivo	Manual	No Redundante y Agrega Vr.	Ocasional	Adecuada	Si	Si	Si	Si	Físico	ACEPTAR
CO10	Seguimiento por parte del administrador del contrato	Preventivo	Manual	No Redundante y Agrega Vr.	Permanente	Adecuada	Si	Si	Si	Si	Magnético y físico	ACEPTAR
CO12	Aprobacion de la recepcion del bien y/o servicio por parte del area solicitante	Preventivo	Semiautomatico	No Redundante y Agrega Vr.	Permanente	Adecuada	Si	Si	Si	Si	Magnético y físico	ACEPTAR
CO13	Verificacion por parte del administrador del contrato que la factura cumpla con los requisitos del pedido	Preventivo	Semiautomatico	No Redundante y Agrega Vr.	Permanente	Adecuada	Si	Si	Si	Si	Magnético y físico	ACEPTAR
CO14	Validacion en SAP del valor del pedido vs lo facturado (limite de tolerancia)	Preventivo	Semiautomatico	No Redundante y Agrega Vr.	Permanente	Adecuada	Si	Si	Si	Si	Magnético y físico	ACEPTAR
CO15	Niveles de aprobacion de pagos autorizados en SAP	Preventivo	Semiautomatico	No Redundante y Agrega Vr.	Permanente	Adecuada	Si	Si	Si	Si	Magnético y físico	ACEPTAR
CO16	Bloqueo y cumplimto de las condiciones de pago pactado	Preventivo	Semiautomatico	No Redundante y Agrega Vr.	Permanente	Adecuada	Si	Si	Si	Si	Magnético y físico	ACEPTAR
	0											ACEPTAR

Imagen creada por autores,

8.3 Diseño de matriz para establecer mapa de controles

En la matriz mapa de controles, se pretende resumir los controles aplicados a los diferentes riesgos asociados a los procesos de la organización, mostrando la descripción, la valoración del diseño de control y la ejecución del control en términos cualitativos, para de esta manera tener presente que medidas de administración tienen falencias y cuales se pueden considerar robustas.

Figura 13. Mapa de controles



MAPA DE CONTROLES

B	C	D
MAPA DE CONTROLES		
CONTROLES O MEDIDA DE ADMINISTRACIÓN	**VALORACION DEL DISEÑO DEL CONTROL**	**VALORACION DE LA EJECUCION DEL CONTROL**
Estatutos de contratacion, la directiva ... manual de contrataciones y un procedimiento de compras de bienes y servicios, codigo de etica, politica de compra a nivel de grupo.	BUENO	Debil
revision y aprobacion del SOLP por el jefe inmediato	BUENO	No se ejecuta
Existencia de un presupuesto aprobado y registrado en SAP	OPTIMO	Fuerte
Registro actualizado de proveedores en el sistema de información SAP	DEFICIENTE	Moderado
Registro de evaluacion y selección de la(s) mejor(es) oferta(s), teniendo en cuenta los requerimientos juridicos, tecnicos y financieros	OPTIMO	Debil
Segregacion de funciones para la elaboracion y revision de los terminos de referencia para que estos concuerden con el contrato	OPTIMO	Moderado
Administración de cambios para la definición y parametrización de BLUEPRINT	OPTIMO	Fuerte
Administracion de roles y permisos por cargos	OPTIMO	Moderado
El area juridico establece las garantias al momento de la elaboracion del contrato	BUENO	Debil
Seguimiento por parte del administrador del contrato	BUENO	Debil

Imagen creada por autores.

8.4 Diseño de matriz para determinar la reducción del riesgo (Efectividad medidas de administración)

Al momento de entregar un informe con respecto a la gestión y administración de riesgos, ésta matriz toma mucha importancia; puesto que es en ésta, donde se resume que tan práctica son las medidas de administración, con respecto a los riesgos inherentes.

Inicialmente se ubican los riesgos puros y residuales, de acuerdo a lo implementado por Transelca S.A ESP en la administración de riesgos estratégicos, en donde se estiman zonas de clasificación de los riesgos, de la siguiente forma:

Figura 14. Zonas de clasificación de los riesgos

Imagen tomada de: Grupo ISA, Transelca S.A. ESP,

Seguidamente, se pasa a ubicar los riesgos puros en cada cuadrante, la intensidad de los colores demarca cada una de las zonas (diseño tomado de lo que Transelca S.A. ESP viene manejando), dependiendo como afecte la probabilidad Vs impacto. De ésta manera, se determina como se encuentra un proceso con respecto a los riesgos inherentes.

Por otro lado, tenemos la ubicación del riesgo residual, es decir, como quedan los riesgos de los procesos tratados con los respectivos controles, mostrando así, que tan robustas son las medidas de administración como para mitigar el riesgo, o por el contrario, hay que emplear controles más adecuados para esos riesgos que se mantienen en zonas diferentes a las aceptables.

Por último, se determina la efectividad de las medidas de administración, realizando una sumatoria del riesgo puro de cada proceso, restando la mitigación que se obtiene al aplicar los respectivos controles, la cual obtenemos en el riesgo residual, y se divide entre todo el conjunto de riesgos sin tratamientos, es decir, se

divide entre el riesgo puro, obteniendo lo que se le llama reducción del riesgo (Efectividad medidas de administración).

Es importante aclarar que éste proceso se lleva a cabo por cada recurso de la organización, es decir, para el caso de Transelca S.A ESP que maneja cuatro recursos claves, se requiere implementar este informe por cada recurso, determinando así, que riesgos los impactan y como se administran.

Figura 15. Reducción del riesgo (efectividad medida de administración)

Imagen creada por autores

8.5 Identificación de riesgos por procesos

Una vez establecida la matriz para gestión y administración de riesgos por proceso, el siguiente paso fue establecer pruebas con datos de Transelca S.A. ESP, identificando los riesgos del proceso, realizando las pruebas con información antes revisada por el departamento de auditoría interna, obteniendo resultados satisfactorios.

La intención de la identificación de riesgos por procesos, es buscar la mayor seguridad posible por parte de la organización, en las actividades principales que día a día se ejecutan, para de esta forma estar siempre competentes y tomar las medidas necesarias en el momento preciso.

8.5.1 Riesgos en el proceso de adquisición de bienes y/o servicios de Transelca S.A ESP

Como se menciono anteriormente, los datos aquí consignados son datos de pruebas de un proceso que se ejecuta en Transelca S.A. ESP, el proceso seleccionado para realizar las primeras pruebas de ésta herramienta dinámica, es el proceso de adquisición de bienes y/o servicios (proceso de Compras).

A continuación, detallamos las pruebas realizadas con la herramienta dinámica para mostrar cómo se comportan, con las diferentes variables previamente definidas.

Inicialmente describimos los riesgos a los que está expuesta la organización en el proceso antes mencionado, seguidamente se evalúa la probabilidad Vs impacto por el dueños del proceso, funcionarios implicados, y el departamento de auditoría interna, obteniendo los valores para el riesgo puro.

Figura 16. Describir riesgos

PROCESO	SUBPROCESO	RIESGO	CLASIFICACION DEL RIESGO	IMPLICACIONES	ETAPAS PHVA
(A12)Administrar y Gestionar la Adquisición de bienes y/o servicios.	(A121) Suscribir Pedidos y Contratos	Incumplimiento de las directivas y normas legales de contratación	1. Ausencia y/o falta de pertinencia de políticas y procedimientos	Sanciones legales, perdida de credibilidad	Verificar
		Solicitud de un bien y/o servicio innecesario o sin justificación	10. Inadecuada asignación de Acceso a usuarios	Sobrecostos, gastos innecesarios a traves de la creacion de SOIP sin autorización para favorecimiento a terceros o beneficios personales	Planear
		Invitar a proveedores que se encuentren registrados en la Lista CLINTON, sancionados, que no sean idóneos, que presenten conflictos de interés y que hayan obtenido bajas calificaciones en la evaluación de proveedores	2. Incumplimiento de políticas y procedimientos	Obtener bienes y/o servicios de baja calidad, sobrecostos, problemas legales y a su vez de imagen perdiendo credibilidad	Planear
		Favorecimiento a proveedores que no cumplan con las mejores condiciones en cuanto a la oferta	12. Fraude	Sobrecosto, calidad deficiente, deterioro de imagen, ausencia de garantía, problemas legales	Hacer
		Omision intencional entre los terminos de referencia y el contrato suscrito entre las partes	12. Fraude	Diferencias desfavorables para la empresa en cuanto a precio, calidad, tiempo, garantia	Verificar
		Inadecuada configuración y/o parametrización del sistema de información SAP	13. Inadecuada configuración / parametrización del sistema	Perdidas economicas, información confidencial en manos de usuarios no autorizados	Actuar
		Inadecuada asignacion de autorizaciones para liberar pedido	12. Fraude	Perdidas economicas por favorecimiento a terceros y/o beneficios personales	Verificar
		Inadecuada gestion de garantia	4. Falta de gestión	Perdidas economicas o de imagen por falta de polizas: buen uso del anticipo, cumplimiento, estabilidad de obra, pago de salarios y prestaciones sociales	Planear
					Planear
		Incumplimiento de proveedores	7. Incumplimientos de proveedores	Perdidas economicas por calidad, retrasos en la entrega del bien y/o servicios, incumplimiento en el pago de la seguridad social	Planear
		Recepcion de bienes y servicios que no cumplan con las especificaciones pactadas	4. Falta de gestión	Perdidas economicas, sobrecostos, implicaciones legales y perdida de imagen	Planear
		Admitir facturas que no cumplan con los requisitos pactados en el contrato	4. Falta de gestión	Detrimento economico	Verificar
		Contabilizar por un monto superior y/o no descontar los anticipos	12. Fraude	Detrimento economico	Verificar
		Pago de facturas ficticias (financieras)	12. Fraude	Detrimento economico	Verificar
		Pago de Facturas antes de la fecha de vencimiento	2. Incumplimiento de políticas y procedimientos	Descontrol de los pagos programados en un periodo determinado	Planear

Imagen creada por autores.

Figura 17. Determinar riesgo puro

FINANCIERO		HUMANO		INFORMACIÓN		IMAGEN		VALORACIÓN RIESGO PURO			
Probab.	Severidad	Probab.	Severidad	Probab.	Severidad	Probab.	Severidad	FINANCIERO	HUMANO	INFORMACIÓN	IMAGEN
Muy Baja	Leve	Baja	Moderado	Media	Crítico	Media	Muy Crítico	1	4	9	12
Baja	Crítico	N/A	N/A	Baja	Moderado	Baja	Moderado	6	N/A	4	4
Alta	Muy Crítico	Muy Baja	Leve	Baja	Moderado	Baja	Moderado	16	1	4	4
Muy Baja	Muy Crítico	N/A	N/A	Media	Crítico	Alta	Muy Crítico	4	N/A	9	16
Baja	Moderado	N/A	N/A	Baja	Leve	Alta	Muy Crítico	4	N/A	2	16
Alta	Crítico	N/A	N/A	Media	Moderado	Alta	Muy Crítico	12	N/A	6	16
Alta	Muy Crítico	N/A	N/A	Alta	Crítico	Baja	Leve	16	N/A	12	2
Media	Muy Crítico	N/A	N/A	Baja	Leve	Media	Moderado	12	N/A	2	6
Muy Baja	Leve	N/A	N/A	Media	Moderado	Alta	Muy Crítico	1	N/A	6	16
Alta	Muy Crítico	N/A	N/A	Media	Moderado	Alta	Muy Crítico	16	N/A	6	16
Media	Crítico	Muy Baja	Crítico	Muy Baja	Leve	Media	Muy Crítico	9	3	1	12
Baja	Crítico	N/A	N/A	Muy Baja	Crítico	Alta	Muy Crítico	6	N/A	3	16
Media	Muy Crítico	N/A	N/A	Baja	Moderado	Baja	Moderado	12	N/A	4	4
Media	Crítico	N/A	N/A	Media	Crítico	Media	Crítico	9	N/A	9	9
Baja	Muy Crítico	N/A	N/A	Media	Muy Crítico	Media	Crítico	8	N/A	12	9
Alta	Crítico	N/A	N/A	Baja	Moderado	Media	Crítico	12	N/A	4	9

Imagen creada por autores

Paso seguido, se procede a determinar las medidas de control, por tal razón, pasamos a determinar que tan robusto es el diseño de dichas medidas, en la matriz correspondiente; luego, se revisa la ejecución de los controles cuantificando los diferentes valores cualitativos que éste tiene, para promediarlos con el diseño del control, obteniendo así el riesgo residual para dicho proceso.

Figura 18. Determinar riesgo residual

TRATAMIENTO DEL RIESGO	CODIGO DEL CONTROL	CONTROL/MEDIDA DE ADMINISTRACION	VALORACION DEL DISEÑO DEL CONTROL	VALORACION DE LA EJECUCION DEL CONTROL		VALORACION RIESGO RESIDUAL			
						FINANCIERO	HUMANO	INFORMACIÓN	IMAGEN
Aceptar	CO1	Manual de contrataciones y un procedimiento de adquisición de bienes y servicios, codigo de etica, politica de compra a nivel de grupo.	3	Debil	2	0,40	1,60	3,60	4,80
Compartir	CO2	revision y aprobacion del SOLP por el jefe inmediato	3	No se ejecuta	1	6,00	N/A	4,00	4,00
Controlar	CO3	Existencia de un presupuesto aprobado y registrado en SAP	4	Fuerte	4	4,00	0,25	1,00	1,00
Aceptar	CO4	Registro actualizado de proveedores en el sistema de información SAP	1	Moderado	3	2,00	N/A	4,50	8,00
Controlar	CO5	Registro de evaluacion y selección de la(s) mejor(es) oferta(s), teniendo en cuenta los requerimientos juridicos, tecnicos y financieros	4	Debil	2	1,33	N/A	0,67	5,33
Aceptar	CO6	Segregacion de funciones para la elaboracion y revision de los terminos de referencia para que estos concuerden con el contrato	4	Moderado	3	3,43	N/A	1,71	4,57
Aceptar	CO7	Administración de cambios para la definición y parametrización de BLUEPRINT	4	Fuerte	4	4,00	N/A	3,00	0,50
Aceptar	CO8	Administracion de roles y permisos por cargos	4	Moderado	3	3,43	N/A	0,57	1,71
Aceptar	CO9	El area juridico establece las garantias al momento de la elaboracion del contrato	3	Debil	2	0,40	N/A	2,40	6,40
Aceptar	CO10	Seguimiento por parte del administrador del contrato	3	Debil	2	6,40	N/A	2,40	6,40
Aceptar	CO10	Seguimiento por parte del administrador del contrato	3	Debil	2	3,60	1,20	0,40	4,80
Aceptar	CO12	Aprobacion de la recepcion del bien y/o servicio por parte del area solicitante	4	Moderado	3	1,71	N/A	0,86	4,57
Aceptar	CO13	Verificacion por parte del administrador del contrato que la factura cumpla con los requisitos del pedido	4	Moderado	3	3,43	N/A	1,14	1,14
Aceptar	CO14	Validacion en SAP del valor del pedido vs lo facturado (limite de tolerancia)	4	Fuerte	4	2,25	N/A	2,25	2,25
Aceptar	CO15	Niveles de aprobacion de pagos autorizados en SAP	4	Moderado	3	2,29	N/A	3,43	2,57
Aceptar	CO16	Bloqueo y cumpliento de las condiciones de pago pactado	4	Moderado	3	3,43	N/A	1,14	2,57

Fig. 18 Creada por autores,

Por último, se determina el estado de riesgos en el proceso de adquisición de bienes y servicio en cada recurso de la organización, estableciendo el estado inicial de cada recurso frente a los riesgos (riesgos puros), y el estado de cada recurso con los riesgos tratados con controles (riesgos residuales), obteniendo la efectividad de las medidas aplicadas. Los resultados obtenidos fueron satisfactorios y se ajustan a la realidad del negocio.

Figura 19.Efectividad medidas de administración. Recurso financiero

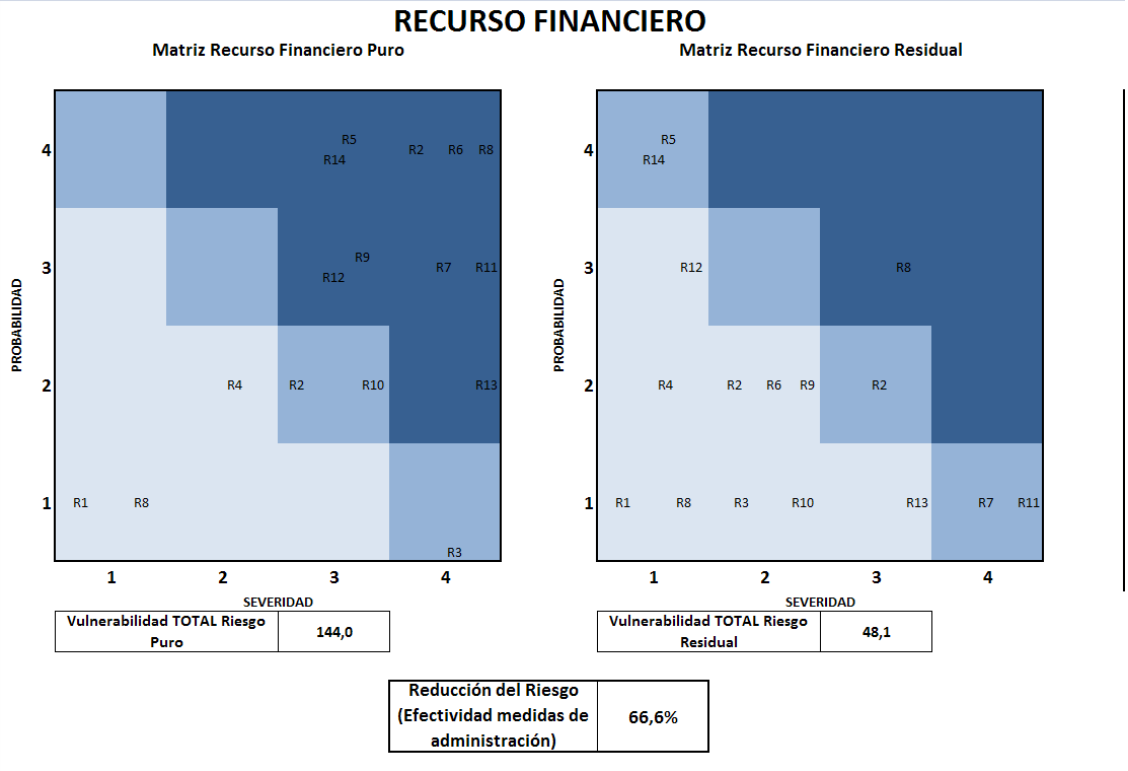


Imagen creada por autores,

Se nota claramente que la reducción del riesgo, realizando el ejercicio con la herramienta, es de 66.6% para el recurso financiero, esta efectividad cambia de acuerdo a cada recurso y a como impactan sobre el proceso al cual se le aplica la gestión y administración de riesgos.

Figura 20. Efectividad medidas de administración recurso humano

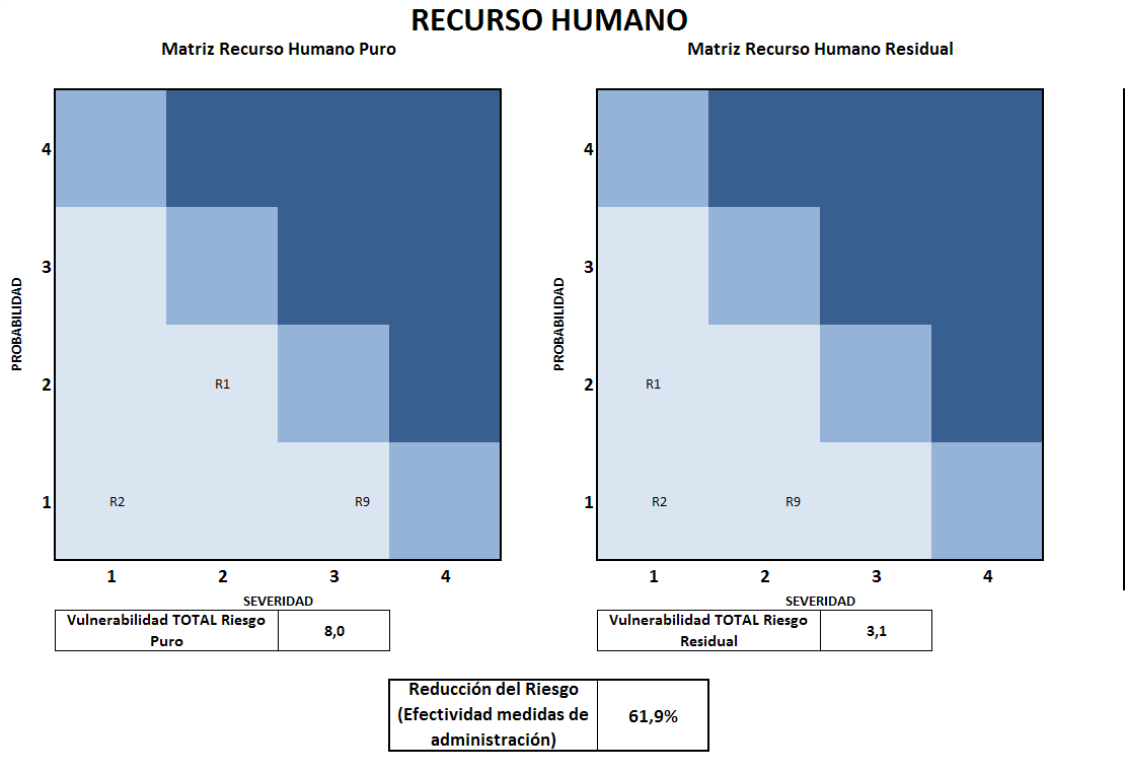


Imagen creada por autores,

Figura 21. Efectividad medidas de administración recurso información

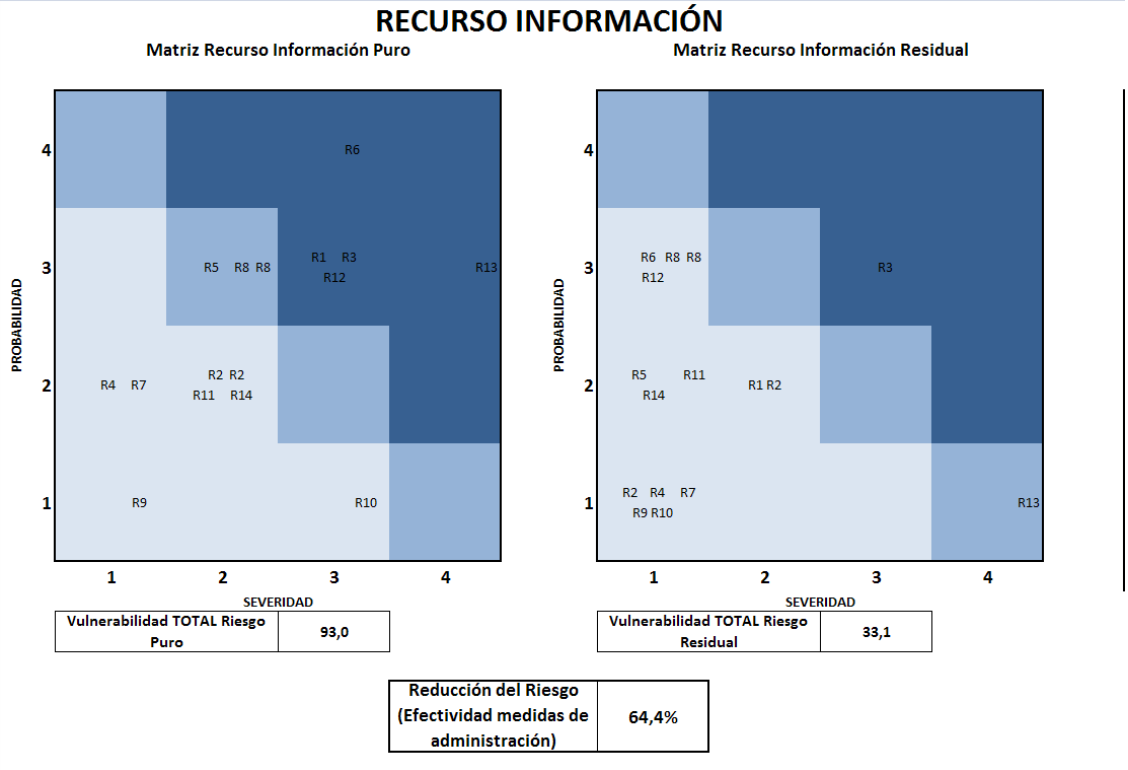


Imagen creada por autores

Figura 22.Efectividad medidas de administración recurso imagen corporativa

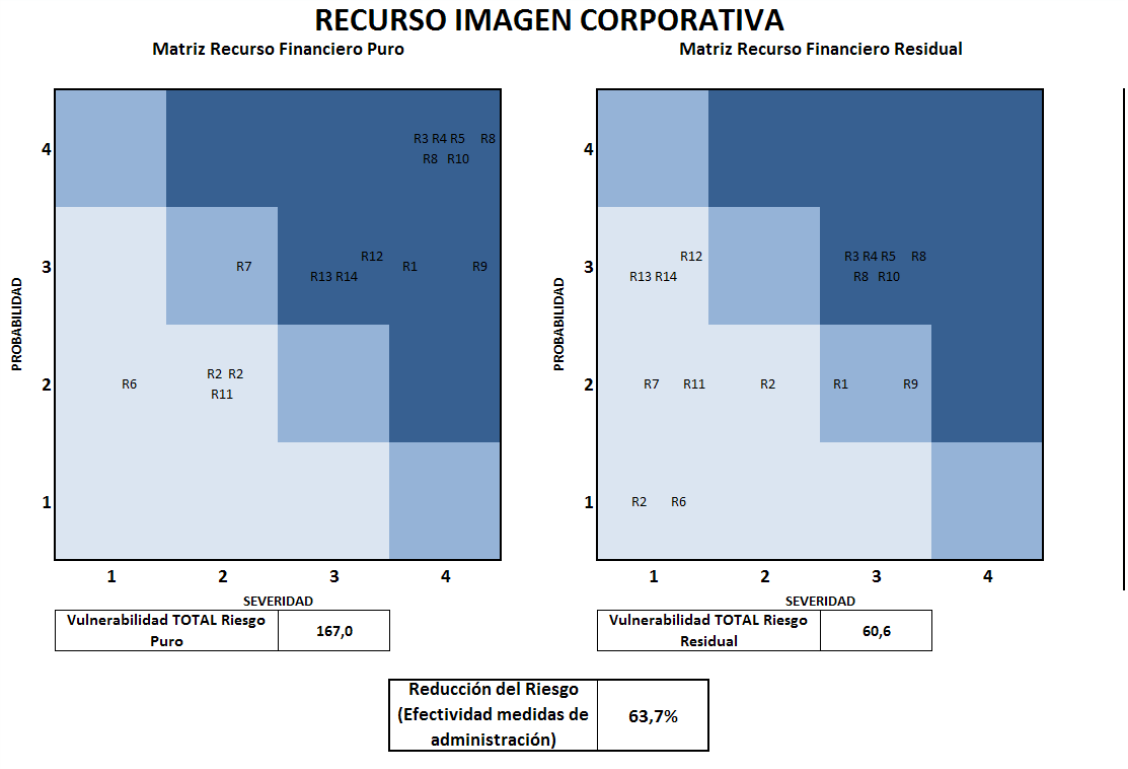


Imagen creada por autores.

9. CONCLUSIONES

Todas las organizaciones con planes de competitividad y expansión a un mercado multinacional, han comprendido la importancia de gestionar y administrar los riesgos inherentes a los diversos procesos ejecutados. En muchas organizaciones se viene trabajando los riesgos que afecten la consecución de los objetivos estratégicos, ubicando de ésta forma, los riesgos estratégicos que pongan en peligro la consecución de los objetivos organizacionales.

Transelca S.A. ESP, no es la excepción a la regla, tienen muy bien definida las diferentes políticas de gestión de riesgos, a tal punto que cuentan con un sistema para dicha gestión, muy claramente definido; el GIR (Gestión Integral de Riesgos): “Implementación sistemática de un conjunto de acciones tendientes al manejo óptimo de los riesgos en todos los procesos. "Este manejo tiene como gran objetivo garantizar la continuidad de los negocios de la organización".

Teniendo en cuenta lo anterior, se diseño e implemento una herramienta dinámica para la gestión y administración de riesgos, que contribuyera de manera objetiva, con la gestión integral de riesgos por procesos, el diseño, acorde a lo trabajado inicialmente por el grupo empresarial ISA, del cual hace parte la empresa, e implementando las diversas variables, en un proceso de alta trascendencia dentro de Transelca S.A. ESP.

En la empresa, la gestión de riesgos, no contaba con antecedentes de herramientas dinámicas para la GIR, por tal razón, se diseña buscando parametrizar los valores previamente definidos e integrando el control interno organizacional, como medidas de tratamiento para mitigación de riesgos.

La herramienta no solo determina el estado de un proceso frente a los riesgos inherentes que éste posea, sino que además, revisa el estado de los controles con respecto al diseño, y la ejecución adecuada para mitigar los riesgos puros por proceso; de esta forma se obtiene un reporte objetivo, de los diferentes recursos de la organización, con respecto a los riesgos que afectan el proceso en ejecución.

Respecto al proceso de adquisición de bienes y/o servicios, se realizo una prueba piloto con los riesgos hallados para dicho proceso y las medidas de administración existentes, para mitigar los riesgos identificados, utilizando de esta manera, los resultados obtenidos como pilar fundamental, para determinar el estado del proceso, obteniendo resultados satisfactorios a las pruebas realizadas, fundamentados en una gran objetividad.

Por tal razón, Transelca S.A. ESP seguirá utilizando la metodología y la herramienta dinámica para identificar, valorar, administrar y gestionar los riesgos, de igual forma las medidas de administración que mitiguen los riesgos determinados por procesos, dejando de lado la subjetividad con la que se venían trabajando los riesgos.

Por lo antes dicho, es importante resaltar, que las organizaciones que invierten esfuerzos en la gestión y administración de riesgos, tienen un paso en frente con respecto al éxito, Transelca S.A. ESP es una organización muy robusta en éste campo de la Gestión Integral de Riesgos, con la herramienta dinámica, se va a fortalecer mucho más en la objetividad de éste tema particular.

10. REFERENCIAS BIBLIOGRAFICAS

AVILA Bustos, Juan. Medición y control de riesgos financieros en empresas del sector real. Tesis (Contador Público). Bogotá, Colombia, Pontificia Universidad Javeriana, facultad de ciencias económicas, administrativas y contables, 2005, 7 p.

Guía para el uso de la norma NTC 5254 gestión del riesgo dentro del proceso de auditoría interna.

Guía de administración del riesgo, Departamento administrativo de la función pública, República de Colombia.

Superintendencia Financiera de Colombia, Circular externa 048 diciembre de 2006: Reglas relativas a la administración del riesgo operativo.

GUTIERREZ Correa, Juan. Sistematización del proceso de gestión integral de riesgos para una empresa administradora del mercado de energía colombiano, Tesis (ingeniero de sistemas y computación). Pereira, Colombia, Universidad Tecnológica de Pereira, facultad de ingenierías, 2008, 18 p.

The Institutes of Internal Auditors Research Foundation (IIARF), Evaluación eficaz del sistema de control interno. 1 ed, Florida, 2008. 21 p. ISBN 978-0-89413-621-4

Alberto Cancelado González. Sistema de administración de riesgos en tecnología informática [citado noviembre de 2003]. Disponible en internet:< URL: http://www.gestiopolis.com/recursos/documentos/fulldocs/ger1/sistecinfor.htm>

Normas generales de control interno [citado el 01 agosto de 1998]. Disponible en internet: < URL: http://www.sigen.gov.ar/documentacion/ngcind.asp>

Apreciación de riesgos [citado 21 julio de 2003]. Disponible en internet: < URL: http://www.ccee.edu.uy/ensenian/catcoint/material/riesgos.PDF>

Pedro Pérez Solórzano. Los cinco componentes del control interno [citado 26 de enero de 2007]. Disponible en internet: <URL: http://www.degerencia.com/articulo/los_cinco_componentes_del_control_interno>

Briseyda Tineo. Auditoría de sistemas [citado 29 julio de 2011]. Disponible en internet: < URL: http://es.scribd.com/doc/61220171/12/b-CONTROLES-DETECTIVOS>

Briseyda Tineo. Auditoría de sistemas [citado 29 julio de 2011]. Disponible en internet: < URL: http://es.scribd.com/doc/61220171/12/b-CONTROLES-CORRECTIVOS>

José Maya. Método de control de proceso [citado 8 octubre 2011]. Disponible en internet: < URL: http://www.unalmed.edu.co/josemaya/Ing_prod/Control%20de%20Proceso-%20Metodo.pdf>